PLANTEAMIENTO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN LA UNIVERSIDAD ECCI PARA EL SISTEMA DE INFORMACIÓN ACADÉMICO ARCA - MÓDULO GRADEBOOK BAJO LA NORMA ISO 27001:2013

OSIRIS YASBLEIDY TORRES GUTIÉRREZ
IVÁN DARÍO CORTÉS ROJAS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

PLANTEAMIENTO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN LA UNIVERSIDAD ECCI PARA EL SISTEMA DE INFORMACIÓN ACADÉMICO ARCA - MÓDULO GRADEBOOK BAJO LA NORMA ISO 27001:2013

OSIRIS YASBLEIDY TORRES GUTIÉRREZ
IVÁN DARÍO CORTÉS ROJAS

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Director:
ING. LORENA OCAMPO CORREA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma presidente del jurado

_____
Firma jurado

_____
Firma jurado

Bogotá D.C. 6 de diciembre de 2016

DEDICATORIA

El proyecto de grado es dedicado a Dios y a las familias de las personas que realizaron el proyecto. A Dios porque ha estado delante del desarrollo del proceso sorteando las dificultades, guiando y multiplicando las fuerzas para no desfallecer. A los hogares de cada miembro que compone el trabajo como los hijos, padres, hermanos, esposos que son motores y la fortaleza para seguir cosechando triunfos profesional para brindar un mejor estilo de vida. A todos y cada uno de los compañeros y amigos cercanos que depositaron su entera confianza en cada reto que se presentó y sin dudar ni un solo momento de la capacidad de los integrantes del proyecto apoyaron la labor ofreciendo su impulso y logística para la culminación del presente proyecto.

AGRADECIMIENTOS

Este proyecto es el resultado del esfuerzo conjunto de un grupo de trabajo (Osiris e Iván), de la Ing. Lorena Ocampo quien incansablemente marco los derroteros para avanzar de manera práctica, clara y finalmente de los compañeros cercanos, que estuvieron acompañando el proceso durante las diferentes materias de la especialización, cada uno de ellos el desarrollo del proyecto aportando sus experiencias y conocimiento.

Se agradece de manera especial a la Universidad ECCI quienes apoyaron de manera incondicional el proyecto y documento con lujo de detalles.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE ILUSTRACIONES

pág.

INTRODUCCIÓN

En el presente trabajo, se planteará un sistema de gestión de la seguridad de información para el módulo de Gradebook (Libro de notas) que se encuentra en el sistema de información académico de la Universidad ECCI - UECCI. Este módulo permite la creación de actividades que se van evaluar a los estudiantes, permitiendo el ingreso, la modificación de las notas parciales y finales por parte del docente que imparte la cátedra. La importancia de este trabajo para la institución es alta debido a que dentro de la visión se evidencia lo siguiente *"Seremos una Universidad reconocida* **por su humanismo y educación tecnológica** *con criterios de universalidad en el conocimiento, con programas pertinentes y de alta calidad,* ***líderes en principios y valores al servicio*** **de la formación del capital humano**" este mensaje muestra claramente como para la Universidad el avance tecnológico es primordial para su constante desarrollo y crecimiento, es por ello que se busca plantear el aseguramiento de la información que se encuentra en el módulo Gradebook proponiendo controles y políticas para proteger uno de los activos más importantes de la Institución como lo son las notas de los estudiantes y que mejor que a través de un sistema de gestión de la seguridad de la información que se encuentra relacionada directamente con las tecnologías.

La información que se almacena en la base de datos hoy en día es un activo muy importante, no solo para la Universidad sino para los usuarios finales (estudiantes, docentes, coordinaciones, administrativos y Ministerio de Educación Nacional), es por este motivo que la misma requiere ser asegurada y protegida en forma apropiada. La información no solo se ve en riesgo por la manipulación del usuario a nivel interior de la UECCI sino que también por la manipulación que se puede presentar a nivel externo. Ningún sistema está 100% seguro y libre de ser atacado, pero con este planteamiento se busca que las notas obtenidas por los estudiantes y cargadas al sistema por el docente cuenten con los tres pilares de la información Integridad, Confidencialidad y Disponibilidad.

1. DEFINCIÓN DEL PROBLEMA

La Universidad ECCI en el año 2012 implementó un sistema académico – financiero llamado PeopleSoft - ARCA, el cual se compone de varios módulos: Comunidad del Campus, Registro e Inscripciones, ***Gradebook***, Finanzas del Campus, Orientación Académica. Para este proyecto se va a trabajar el modulo "*Gradebook*", en este módulo el docente registra las notas (parciales y definitivas) de las materias cursadas por los estudiantes durante un periodo académico en la Universidad.

El docente encuentra parametrizado el sistema con los tres cortes que ha estipulado la Universidad para evaluar a un estudiante, el docente solo debe realizar el cargue de notas de cada corte, las notas pueden ser cargadas dentro del rango de fechas parametrizados previamente en el sistema para la apertura y cierre de ciclo lectivo. La Pregunta es ¿Cómo mejorar la confidencialidad, integridad y disponibilidad de las notas reportadas en el sistema ARCA?

La Universidad tiene estipulado los porcentajes de cada corte que se realiza en la academia para valorar los conocimientos de los estudiantes los cuales se componen de los siguientes (30% - primer corte, 30% - segundo corte y 40% - tercer corte)[1], cada docente cuenta con la autonomía de asignar tantas actividades como desee para evaluar cada uno de esos cortes pero al final de cada corte solo debe cargar una única nota en el sistema. Hoy en día los docentes no entregan soporte de las notas cargadas en el sistema, se evidencia un riesgo en la integridad de la Información debido a que esta puede ser manipulada después de ser cargada y notificada en el sistema y no existe un soporte impreso o medio magnético de las notas cargas durante el periodo lectivo con el cual comparar la nota real.

[1] UNIVERSIDAD ECCI. Artículo 45: De la seriedad de las pruebas acádemicas. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. p. 38.

2. JUSTIFICACIÓN

Actualmente la Universidad ECCI es una Institución de Educación Superior para formar profesionales íntegros, reconocidos por su lema “humanismo y educación tecnológica y con un servicio de alta calidad”[2]. Como su misión y visión lo indican uno de los temas principales es la calidad, es por eso que se debe empezar a velar por la calidad de la información que se registra, almacena y mantiene en el sistema de información académico ARCA, para este trabajo más exactamente el registro de notas de los estudiantes que es el módulo de Gradebook.

Hoy en día UECCI, no cuenta con un sistema de gestión de seguridad de la información que garantice de forma medible la integridad y disponibilidad de la información. Teniendo en cuenta que las notas son uno de los activos de información principal de la Universidad es evidente la necesidad de plantear un sistema de gestión de seguridad de información para su futura implementación en este módulo, debido a que este permite identificar y evaluar los riesgos, las amenazas y las vulnerabilidades.

El sistema de Gestión de Seguridad de la Información planteado en este proyecto se basará en la Norma ISO 27001:2013, el cual contempla entre otros los procedimientos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La UECCI actualmente se encuentra realizando gestión con la empresa Certificadora ICONTEC para realizar la capacitación al personal que pertenece al departamento de Dirección TIC en la norma mencionada con el fin de iniciar la implementación de un sistema de Gestión de la Seguridad de Información en toda la Universidad, este trabajo será la base para la implementación de la Norma.

[2] UNIVERSIDAD ECCI. Nuestra Misión y Visión. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. p. 5.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Plantear un Sistema de Gestión de Seguridad de Información para el módulo Gradebook en el sistema académico ARCA de la Universidad ECCI bajo la norma ISO 27001:2013

3.2 OBJETIVOS ESPECÍFICOS

- Levantamiento de información de los activos de información módulo Gradebook del sistema académico.

- Realizar el análisis y gestión de riesgos de los activos relacionados con el módulo Gradebook utilizando la metodología MAGERIT V3.0.

- Plantear controles bajo la norma ISO 27001:2013 para mitigar los riegos hallados.

- Generar la política de seguridad de información para los activos más significativos del módulo Gradebook en el Sistema Académico.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En la Universidad ECCI se implementó la herramienta de Oracle *PeopleSoft Campus Solutions* con el fin de organizar la información de todas las áreas de gestión relacionadas con la academia. Esta plataforma tecnológica permite gestionar toda la información de los alumnos, el personal docente, administrativos, inscripciones, admisiones, Calificaciones.

Se han implementado seis módulos de esta plataforma los cuales son: Autoservicio de Campus, Comunidad del Campus, **Libro de notas *(Gradebook)*,** Finanzas del Alumnado, Orientación Académica, Registro del Alumnado. El proyecto se va a enfocar en el módulo *Gradebook* (Libro de notas), éste es un módulo adicional para digitar las notas parciales, dado que las calificaciones definitivas de los estudiantes se pueden cargar en el módulo de registro del alumno. En Gradebook se realiza detalladamente la carga de calificaciones que un estudiante ha obtenido en una materia cursada durante un ciclo lectivo específico, el modulo permite que el docente sea autónomo en asignar las actividades que va a evaluar por corte durante el semestre o trimestre, respetando los valores asignados por la Universidad para cada corte (30% - primer corte, 30% - segundo corte y 40% - tercer corte)[3].

Gradebook[4]:

Ofrece la posibilidad de contar con una bitácora de evaluaciones institucionales durante el ciclo lectivo de un estudiante, el docente es quien realiza el registro de las calificaciones en cada actividad y el estudiante visualiza su desempeño en las materias cursadas.

Beneficios:

- Visualización de resultados de evaluaciones por parte de los alumnos.
- Registro de notas parciales por parte del docente.

[3] UNIVERSIDAD ECCI. Artículo 35: Valoración de una asignatura o curso. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. p. 34.

[4] INTERSERVICES. S.f Cuaderno de Evaluación (Gradebook). [En línea]. <http://interservices.grupodatco.com/soluciones/campus-solutions/cuaderno-de-evaluacion/>.

- Seguimiento del progreso de aprendizaje a través de actividades en el curso.

- Recordatorio de vencimiento de entrega de actividades en el curso.

- Recordatorio de vencimiento de entrega de notas parciales y finales.

- Optimiza la comunicación entre alumnos y docente.

Parametrización del docente: (configuración de actividades)

- Crear las actividades de primer, segundo y tercer corte, estas actividades representan las notas parciales obtenidas por el estudiante.

- Asignación de porcentaje a cada actividad por corte.

- Fechas de inicio y vencimiento de cada actividad.

Registro de notas por el docente:

- Introducción de las notas obtenidas de los estudiantes en las actividades realizadas.

- Seguimiento y modificaciones de las calificaciones obtenidas.

Sistema de Gestión de Seguridad de la Información (SGSI) – en ingles *Information Security Management System, ISMS).*

Basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. Nota: el sistema de gestión incluye la estructura organizacional, las políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.[5]

Antes de iniciar a explicar SGSI, se debe conocer la diferencia entre Seguridad Informática y Seguridad de Información.

[5] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Términos y Definiciones. En: Tecnología de la información. Técnicas de seguridad. Sitemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2006, 3-4 p. (NTC-ISO/IEC 27001).

- **Seguridad Informática:** Protección de las infraestructuras de las tecnologías de la información y comunicación que soportan el negocio[6].

- **Seguridad de la Información:** "Preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad"[7].

Entre los diferentes tipos de activos de información se pueden encontrar los siguientes: correos electrónicos, páginas web, bases de datos, faxes, contratos, presentaciones, documentos entre otros. También se debe tener en cuenta el ciclo de vida de la información debido a que para la UECCI hoy es crítico puede dejar de tener importancia con el tiempo.

La metodología que se va a plantear permite en primer lugar realizar un inventario de activos de información relacionados con el módulo Gradebook, en segundo lugar permite realizar el análisis del riesgo y así poder identificar cual activo esta con mayores (vulnerabilidades, amenazas y nivel de riesgo en el cual se encuentra), en tercer lugar se realizara un tratamiento del riesgo basados en la Norma ISO 27001:2013 trabajando los 114 controles que maneja la norma en el anexo A. Y por último se plantean políticas para que la Universidad las pueda implementar y así pueda medir la eficacia de las medidas tomadas.

- **Gestión del riesgo:** "Son las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo"[8], este proceso permite a través del SGSI, preservar la confidencialidad, integridad y disponibilidad de la misma, en el interior de la Universidad, clientes externos y diferentes entes interesados en la misma.

- **Confidencialidad: "**Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"[9].

- **Integridad: "**Propiedad de salvaguardar la exactitud y estado completo de los activos"[10].

---

[6] ABANTO, Hermes. Modelo de proyectos de tesis. 2015. Trabajo de grado. Disponible en: <http://proyectosingesistemas1.blogspot.com.co/>.
[7] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Op. Cit., p. 3.
[8] Ibíd., p. 3.
[9] Ibíd., p. 3.
[10] Ibíd., p. 3.

- **Disponibilidad: "**Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada"[11].

Con el fin de proporcionar un marco de gestión de la seguridad de la información aplicable para cualquier organización, se ha creado un conjunto de estándares bajo el nombre ISO-IEC 27000, este compendio ayuda a las organizaciones a difundir, implementar las prácticas de seguridad de la información y a tomar conciencia de la importancia de proteger uno de los activos más valiosos que se tienen hoy en día, como lo es la información[12].

Hoy en día el mundo se encuentra en una era en que la información es el activo más preciado para las empresas e incluso para nuestra vida cotidiana, se puede decir que causa más impacto en una empresa el daño de un servidor que un robo a sus instalaciones; con la inclusión de nuevas tecnologías y la masificación de la información viajando por diferentes canales, se hace evidente que el perfil de riesgos para las personas y empresas también cambia, incrementando el nivel de riesgos de la información en sus tres aspectos fundamentales: disponibilidad, integridad y confidencialidad.

Es por esto, que las empresas de ahora cuentan con áreas especializadas en la mitigación de los riesgos elaborando estrategias tales como los planes para la gestión de dichos riesgos totalmente alineados al plan estratégico del negocio.

Teniendo en cuenta este preámbulo, este proyecto se apoyó en avances de los planes de gestión de riesgos ya aplicados en algunas empresas siguiendo como directriz la norma ISO 27001:2013 la cual suministra directrices para la gestión de riesgos.

Aunque las normas ISO son el estándar internacional, no se dejaron de lado otras metodologías de análisis de riesgos, como es el caso de MAGERIT, la cual se detalla en el diseño metodológico que aplico para el desarrollo de este trabajo, esta metodología de análisis de riesgos se complementa con la norma ISO27001:2013, para la aplicación de controles relacionados en el Anexo A de la norma.

[11] Ibíd., p. 2.
[12] Instituto Colombiano de Normas Técnicas y Certificación. Protocolo. En: Compendio Sistema de Gestión de la Seguridad de la Información. 1 ed. Bogotá, D.C.: ICONTEC. 2006.

Seguridad de la Información:

La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno de negocios cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

La información pude existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera que sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funcionales de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen los objetivos específicos de seguridad y del negocio de la organización. Esto debe hacerse en conjunto con otros procesos de gestión del negocio.[13]

- **Análisis del riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo de datos, para determinar la importancia del riesgo.[14]

[13] ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (NORMA ISO/IEC 27000).
[14] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Op. Cit., p. 3.

- **Amenaza:** Causa potencial de un incidente no sedeado, que puede ocasionar daño a un sistema u organización[15].

- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser aprovechada por una o más amenazas.

Riesgo en la seguridad de la información: potencial de que una amenaza explote las vulnerabilidades de un activo, causando daño a la organización[16].

Gestión de riesgos: "La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo."[17], en el mismo sentido "La gestión del riesgo permite analizar procesos para obtener una visión global de la organización y con ello el apoyo requerido por parte de la alta gerencia (al mostrar la necesidad de proteger y gestionar procesos críticos que afecten drásticamente a la organización).

La realización de un análisis de riesgos en el entorno de las Tecnologías de la Información y las Comunicaciones (TIC) proporciona a las organizaciones una visión de la situación, tanto por lo que hace a nivel de protección de sus sistemas de información, como por la relación entre estos niveles y el coste que representa para la organización. De esta forma, la gestión del riesgo se constituye como uno de los pilares fundamentales que permite conocer de manera detallada la infraestructura y su funcionamiento interno, así como las consecuencias de una eventual vulnerabilidad o pérdida de servicio."[18].

---

[15] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Términos y Definiciones. En: Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Bogotá D.C: ICONTEC, 2007, 3 p. (NTC-ISO/IEC 27002).

[16] SECUREIT–IT. Métodos de seguridad para la información digital. [En línea]. <https://www.secureit.es/metodos-de-seguridad-para-la-informacion-digital/> [citado en 2016].

[17] Gestión de Riesgo en la Seguridad Informática https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

[18] SEGURIDAD & TECNOLOGÍA http://blog.siete24.com/gestion-del-riesgo-en-seguridad-metodos-y-herramientas-manejo-de-la-informacion

4.1.1 MAGERIT V 3.0[19]. Acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, es una metodología para el análisis y la gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica CSAE. Esta metodología es abierta al público y cualquier persona puede hacer uso de la misma sin necesidad de solicitar autorización del Ministerio de Administraciones Publicas de España.

Actualizada en 2012 a la versión 3.0 consta de tres libros:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas

Los tres libros son gratuitos y se pueden encontrar en el sitio web del Portal de Administración Electrónica de España.

Consta de 5 pasos documentados y argumentados de forma muy clara para realizar el análisis de riesgos. De esta forma reduce la generación de posibles dudas o vacíos que se puedan presentar en el momento del desarrollo.

Separa el proceso de análisis del proceso de gestión, enfocándose en los resultados del primero para hacer uso de estos en la parte evaluativa de los riesgos.

Es una metodología de uso público, es decir se puede hacer uso de ella sin ningún problema. Adicional está disponible para descargar los tres libros de forma gratuita y en español. (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., 2012), esta metodología es ideal para empresas que no tienen experiencia o conocimiento en la gestión de riesgos de la información.

Se encuentra alineado a los estándares que imparten las normas ISO y se puede convertir en la base para una futura certificación.

[19] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro I – Método. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012. 22. p.

A continuación, se presenta el método de análisis de riesgo con los conceptos de paso a paso[20]

4.1.1.1 Paso 1 Activos. Determinar los activos más importantes para la empresa, su valor y nivel de criticidad en caso de que se vea afectado.

MAGERIT categoriza los activos de Información en 12 tipos de Activos los cuales se exponen a continuación.

- Activos esenciales (**AE**)[21]

Dícese de aquellos que son esenciales para la supervivencia de la organización; es decir que su carencia o daño afectaría directamente a la existencia de la organización, ver cuadro 1.

Cuadro 1. Activos esenciales

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Esenciales	Datos de carácter personal Datos clasificados	**AE**

Fuente: Autores.

- Activos de arquitectura del sistema (**AA**)[22]

Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior, ver cuadro 2.

[20] Ibíd., p. 22
[21] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro II – Catálogo de elementos. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012. 7. p.
[22] Ibíd., p. 8.

Cuadro 2. Activos de arquitectura del sistema

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Arquitectura del sistema	Punto de acceso al servicio Punto de interconexión Proporcionado por terceros	**AA**

Fuente: Autores.

- Activos de datos e información (**AD**)[23]

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos, ver cuadro 3.

Cuadro 3. Activos de datos / información

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Datos/información	Ficheros Copias de respaldo Datos de configuración Datos de gestión interna Credenciales (password) Datos de validación de credenciales Datos de control de acceso Registro de actividad Código fuente Código ejecutable Datos de prueba	**AD**

Fuente: Autores.

[23] Ibíd., p. 8.

- Activos de claves criptográficas **(AK)**[24]

La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos, ver cuadro 4.

Cuadro 4. Activos de claves criptográficas

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Claves criptografícas	Protección de la información Claves de cifra Claves de firma Protección de las comunicaciones Cifrado de soportes de información Certificados de clave pública	**AK**

Fuente: Autores.

- Activos de servicios **(AS)**[25]

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema, ver cuadro 5.

[24] Ibíd., p. 9.
[25] Ibíd., p. 9.

Cuadro 5. Activos de servicios

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Servicios	Anónimo (sin requerir identificación del usuario) Al público en general (sin relación contractual) A usuarios externos (bajo una relación contractual) Interno (a usuarios de la propia organización) World wide web Acceso remoto a cuenta local Correo electrónico Almacenamiento de ficheros Transferencia de ficheros Intercambio electrónico de datos Servicio de directorio Gestión de identidades Gestión de privilegios PKI - infraestructura de clave pública	**AS**

Fuente: Autores.

- Activos de software aplicaciones informáticas **(ASW)**[26]

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios, ver cuadro 6.

Es preocupante en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

[26] Ibíd., p. 10.

Cuadro 6. Activos de software

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Software	Desarrollo propio Desarrollo a medida Estándar Navegador web Nervidor de presentación Servidor de aplicaciones Cliente de correo electrónico Servidor de correo electrónico Servidor de ficheros Sistema de gestión de bases de datos Monitor transaccional Ofimática Anti-virus Sistema operativo Gestor de máquinas virtuales Servidor de terminales Sistema de backup	**ASW**

Fuente: Autores.

- Activos de equipamiento informático - hardware (**AHW)**[27]

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas, responsables del procesado o de la transmisión de datos, ver cuadro 7.

[27] Ibíd., p. 10.

Cuadro 7. Activos de equipamiento informático (hardware)

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Equipamiento informático	Equipos medios Informática personal Informática móvil Agendas electrónicas Equipo virtual Equipamiento de respaldo Periféricos Medios de impresión Escáneres Dispositivos criptográficos Dispositivo de frontera Soporte de la red Módems Concentradores Conmutadores Encaminadores Pasarelas Cortafuegos Punto de acceso inalámbrico Centralita telefónica Teléfono IP	**AHW**

Fuente: Autores.

- Activos de redes de comunicaciones **(ACOM)**[28]

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro, ver cuadro 8.

[28] Ibíd., p. 11.

Cuadro 8. Activos de redes de comunicaciones

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Redes de comunicaciones	Red telefónica RDSI (red digital) X25 (red de datos) ADSL Punto a punto Comunicaciones radio Red inalámbrica Telefonía móvil Por satélite Red local Red metropolitana Internet	**ACOM**

Fuente: Autores.

- Activos de soportes de información **(AMEDIA)**[29]

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo, ver cuadro 9.

[29] Ibíd., p. 12.

Cuadro 9. Activos de soporte de información

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Soportes de información	Electrónicos Discos Discos virtuales Almacenamiento en red Disquetes Cederrón (CD-ROM) Memorias USB DVD Cinta magnética Tarjetas de memoria Tarjetas inteligentes No electrónicos Material impreso Cinta de papel Microfilm Tarjetas perforadas	**AMEDIA**

Fuente: Autores.

- Activos de equipamiento auxiliar **(AAUX)**[30]

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos, ver cuadro 10.

[30] Ibíd., p. 12.

Cuadro 10. Activos de equipamiento auxiliar

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Equipamiento auxiliar	Fuentes de alimentación Sistemas de alimentación ininterrumpida Generadores eléctricos Equipos de climatización Cableado Cable eléctrico Fibra óptica Robots De cintas De discos Suministros esenciales Equipos de destrucción de soportes de información Mobiliario: armarios, etc Cajas fuertes	**AAUX**

Fuente: Autores.

- Activos de instalaciones **(AL)**[31]

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones, ver cuadro 11.

[31] Ibíd., p. 13.

Cuadro 11. Activos de instalaciones

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Instalaciones	Recinto Edificio Cuarto Plataformas móviles Vehículo terrestre: coche, camión, etc. Vehículo aéreo: avión, etc. Vehículo marítimo: buque, lancha, etc. Contenedores Canalización Instalaciones de respaldo	**AL**

Fuente: Autores.

- Activos de personal **(AP)**

En este epígrafe aparecen las personas relacionadas con los sistemas de información, ver cuadro 12.

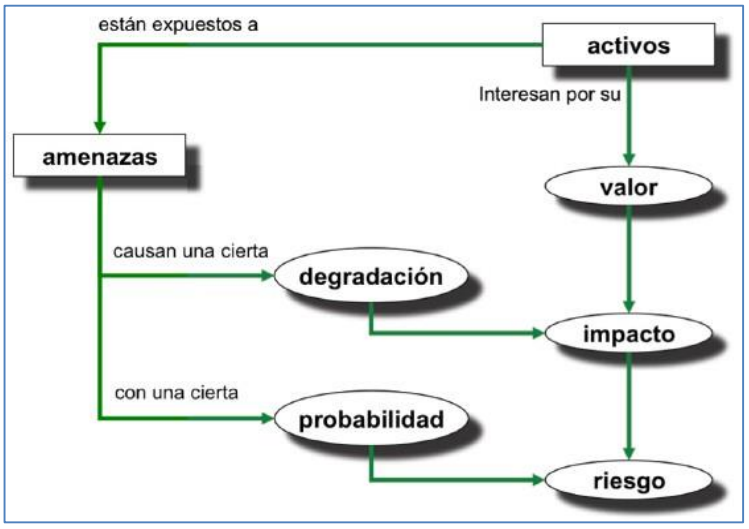
Cuadro 12. Activos de personal

Clasificación de los activos según Magerit V3		
Tipo de activos	***Activo***	***Sigla***
Personal	Usuarios externos Usuarios internos Operadores Administradores de sistemas Administradores de comunicaciones Administradores de bd Administradores de seguridad Desarrolladores / programadores Subcontratas Proveedores	**AP**

Fuente: Autores.

Para determinar el riesgo es necesario evaluar (las amenazas, vulnerabilidades, probabilidades e impactos) siguiendo los pasos como lo propone Magerit, ver la ilustración 1, donde se evidencia la secuencia para realizar un análisis de riesgos.

Ilustración 1. Elementos del análisis de riesgos potenciales



Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, 2012.

4.1.1.2 Paso 2 Amenazas **(AM)**. Determinar las amenazas que pueden llegar a afectar los activos identificados en el paso anterior. Se debe tener en cuenta no solo factores internos sino también ajenos a la organización.

MAGERIT categoriza las amenazas en 4 grandes grupos[32]:

- De Desastres Naturales
- De Origen Industrial
- Fallas en las aplicaciones
- De origen Humano

[32] Ibíd., p. 25.

- **Amenazas desastres naturales**

Nadie esta excepto de los accidentes naturales, ejemplo el sistema de información es víctima pasiva de un desastre natural que se puede ver afectado por un terremoto, inundación entre otros que se evidencian en el cuadro 13.

Cuadro 13. Amenazas de tipo desastre naturales

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM1	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	AHW - AMEDIA - AAUX- AL	Disponibilidad
AM2	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	AHW - AMEDIA - AAUX- AL	Disponibilidad
AM3	Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras. etc.	AHW - AMEDIA - AAUX- AL	Disponibilidad

Fuente: Autores.

- **Amenazas de origen industrial**

El sistema de información es víctima pasiva en caso de un desastre industrial debido a que ve afectado si ocurriese un fallo eléctrico o contaminación electromagnética o cualquier otro desastre que se muestra en el cuadro 14.

Cuadro 14. Amenazas de tipo origen industrial

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM4	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	AHW - AMEDIA - AAUX- AL	Disponibilidad
AM5	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	AHW - AMEDIA - AAUX- AL	Disponibilidad
AM6	Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico.	AHW - AMEDIA - AAUX- AL	Disponibilidad
AM7	Contaminación mecánica	Vibraciones, polvo, suciedad.	AHW - AMEDIA - AAUX	Disponibilidad
AM8	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta	AHW - AMEDIA - AAUX	Disponibilidad
AM9	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	ASW - AHW - AMEDIA - AAUX	Disponibilidad
AM10	Corte del suministro eléctrico	Cese de la alimentación de potencia	AHW - AMEDIA - AAUX	Disponibilidad

Fuente: Autores.

Cuadro 14. Amenazas de tipo origen industrial (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM11	Condiciones inadecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.	AHW - AMEDIA - AAUX	Disponibilidad
AM12	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	ACOM	Disponibilidad
AM13	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante	AAUX	Disponibilidad
AM14	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo	AMEDIA	Disponibilidad

Fuente: Autores.

Cuadro 14. Amenazas de tipo origen industrial (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM15	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés "Transient Electromagnetic Pulse Standard"). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.	AHW - AMEDIA - AAUX- AL	Confidencialidad

Fuente: Autores.

- **Errores y fallos no intencionados**

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión, en el cuadro 15 se describen las posibles amenazas de este tipo.

Cuadro 15. Amenazas de tipo errores y fallos no intencionados

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM16	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	AD, AK, AS, ASW, AMEDIA	Integridad Confidencialidad Disponibilidad
AM17	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	AD, AK, AS, ASW, AHW, ACOM, AMEDIA	Integridad Confidencialidad Disponibilidad
AM18	Errores de monitorización (Log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.	AD log	Integridad
AM19	Errores de configuración	Introducción de datos de configuración erróneos. prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	AD	Integridad
AM20	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	AP	Disponibilidad
AM21	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	ASW	Integridad Confidencialidad Disponibilidad

Fuente: Autores.

Cuadro 15. Amenazas de tipo errores y fallos no intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM22	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	AS, ASW, ACOM	Confidencialidad
AM23	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos	AS, ASW, ACOM	Integridad
AM24	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.		Confidencialidad
AM25	Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	AD, AK, AS, ASW, ACOM, AMEDIA, AL	Integridad
AM26	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	AD, AK, AS, ASW, ACOM, AMEDIA, AL	Disponibilidad

Fuente: Autores.

Cuadro 15. Amenazas de tipo errores y fallos no intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM27	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	AD, AK, AS, ASW, ACOM, AMEDIA, AL, AP	Confidencialidad
AM28	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	ASW	Integridad Confidencialidad Disponibilidad
AM29	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	ASW	Integridad Disponibilidad
AM30	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	AHW, AMEDIA, AAUX	Disponibilidad
AM31	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	AS, AHW, ACOM	Disponibilidad
AM32	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	AHW, AMEDIA, AAUX	Disponibilidad Confidencialidad
AM33	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.	AP	Disponibilidad

Fuente: Autores.

- **Ataques intencionados**

Estos ataques se pueden presentar con fines de beneficiarse a una persona o empresa, también con el ánimo de causar daños y perjuicios a los legítimos propietarios, en el cuadro 16 se presentan algunos de esos ataques.

Cuadro 16. Amenazas de tipo ataques intencionados

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM34	Manipulación de los registros de actividad (log)	Manipulación de los logs.	AD	Integridad
AM35	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento.	AD	Integridad Confidencialidad Disponibilidad
AM36	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	AD, AK, AS, ASW, ACOM	Confidencialidad Autenticidad Integridad
AM37	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	AD, AK, AS, ASW, AHW, ACOM	Integridad Confidencialidad Disponibilidad

Fuente: Autores.

Cuadro 16. Amenazas de tipo ataques intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM38	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	AS, ASW, AHW, ACOM AMEDIA, AAUX, AL	Integridad Confidencialidad Disponibilidad
AM39	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	ASW	Integridad Confidencialidad Disponibilidad
AM40	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	AS, ASW,ACOM	Confidencialidad

Fuente: Autores.

Cuadro 16. Amenazas de tipo ataques intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM41	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	AS, ASW, ACOM	Integridad
AM42	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	AD, AK, AS, ASW, AHW, ACOM, AMEDIA, AAUX, AL	Confidencialidad Integridad
AM43	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.	ACOM	Confidencialidad
AM44	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	AS, AD log	Integridad
AM45	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	AD, AK, AS, ASW, ACOM, AMEDIA, AL	Integridad

Fuente: Autores.

Cuadro 16. Amenazas de tipo ataques intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM46	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	AD, AK, AS, ASW, AMEDIA, AL	Disponibilidad
AM47	Divulgación de información	Revelación de la Información	AD, AK, AS, ASW, ACOM, AMEDIA, AL	Confidencialidad
AM48	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	ASW	Integridad Confidencialidad Disponibilidad
AM49	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	AHW, AMEDIA, AAUX	Confidencialidad Disponibilidad
AM50	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	AS, AHW, ACOM	Disponibilidad

Fuente: Autores.

Cuadro 16. Amenazas de tipo ataques intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM51	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	AHW, AMEDIA, AAUX	Confidencialidad Disponibilidad
AM52	Ataque destructivo	Vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	AHW, AMEDIA, AAUX AL	Disponibilidad
AM53	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	AL	Confidencialidad Disponibilidad

Fuente: Autores.

Cuadro 16. Amenazas de tipo ataques intencionados (Continuación)

Clasificación de las amenazas según Magerit V3				
ID	**Categorías**	**Descripción**	**Activos que puede afectar**	**Dimensión**
AM54	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos	AP	Disponibilidad
AM55	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	AP	Integridad Confidencialidad Disponibilidad
AM56	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	AP	Integridad Confidencialidad Disponibilidad

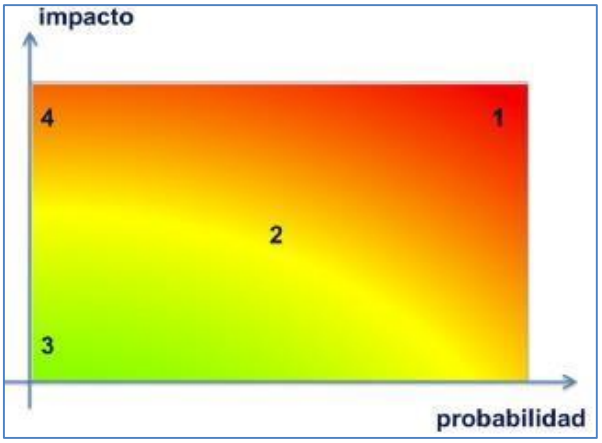
Fuente: Autores.

Una vez se identifican y se clasifican las amenazas se debe valorar en qué grado puede afectar el activo, a esto se le conoce como impacto potencial. Se usan los criterios de probabilidad e impacto. En ambos casos se pueden usar métricas, por ejemplo, para determinar la probabilidad es más cómodo usar una métrica cuantitativa que representaría la frecuencia de ocurrencia. Para el caso del impacto al activo se usa una métrica cualitativa que da una escala de muy alta a muy baja[33].

[33] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro I – Método, Op. cit. p. 28

En la ilustración 2, se observa el riesgo en función del nivel de impacto y la probabilidad de ocurrencia, también se nota que entre mayor sea la valoración del impacto y más probabilidades tenga de suceder, el riesgo aumenta.

Ilustración 2. El riesgo en función del impacto y la probabilidad



Fuente: Ministerio De Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, 2012[34].

En la ilustración 2 cada número corresponde a una zona:

- **Zona 1:** riesgos críticos con probabilidad e impacto muy alto.
- **Zona 2:** riesgos con situaciones improbables y de impacto medio o riesgos muy probables, pero de impacto bajo o muy bajo.
- **Zona 3:** riesgos improbables y de impacto bajo.
- **Zona 4:** riesgos improbables, pero de impacto muy alto[35].

Se tienen en cuenta los siguientes aspectos antes del Paso 3 salvaguardas, en el caso que no hubiese controles implementados:

Impacto potencial: Es el nivel de degradación del activo por causa de la materialización de una determinada amenaza, se aclara que, aunque una misma

[34] Ibíd., p. 30.
[35] Ibíd., p. 30.

amenaza afecte a más de un activo, su nivel de degradación o impacto puede ser diferente. Lo anterior debido a que no todos los activos tienen el mismo valor y hay unos más importantes para la organización que otros. Para calcular el impacto potencial por lo general se emplea una escala en la que se determina el nivel de degradación del activo. Dicha escala se aplica por cada amenaza y a su vez por cada activo[36].

Riesgo potencial: El riesgo potencial se calcula con base al impacto potencial que genera una amenaza y su probabilidad de ocurrencia. Tomando estas dos variables se puede decir que entre más alto sea el impacto y más probable sea la ocurrencia más crítica será el riesgo. Sin embargo, para medir el riesgo se emplea un mapa de calor en el cual se ubican los niveles resultantes del impacto potencial y la probabilidad, su ubicación determinara la zona de riesgo y por lo tanto el nivel del mismo.

4.1.1.3. Paso 3. Salvaguardas. Este paso consiste en determinar que salvaguardas o controles existen actualmente en la organización y verificar su nivel de eficacia frente al riesgo.

Una vez determinado el nivel del riesgo potencial, se debe hacer la verificación de que salvaguarda de los que se identificaron, hace que el riesgo se mitigue o por lo menos su nivel baje. La efectividad de la salvaguarda puede darse de dos formas, la primera reduciendo la probabilidad de las amenazas y la segunda limitando el daño causado al activo.

Las salvaguardas pueden prestar distintos tipos de protección dependiendo del activo, los más comunes son: preventivo, defectivo, correctivo y disuasivo. Sin embargo, para obtener un abanico más amplio de controles, en el capítulo 6 del libro II “Catalogo de elementos” se detallan los más adecuados para cada tipo de activo.

4.1.1.4. Paso 4. Impacto Residual. Se define como el daño sobre el activo debido a la materialización de la amenaza aun existiendo las salvaguardas, es decir pasó de impacto potencial a impacto residual. Para calcularlo se debe realizar el mismo procedimiento que se usó para hallar el impacto potencial, con la diferencia que se le debe aplicar la efectividad del control, con esto logra que la degradación del activo disminuya o sea nula.

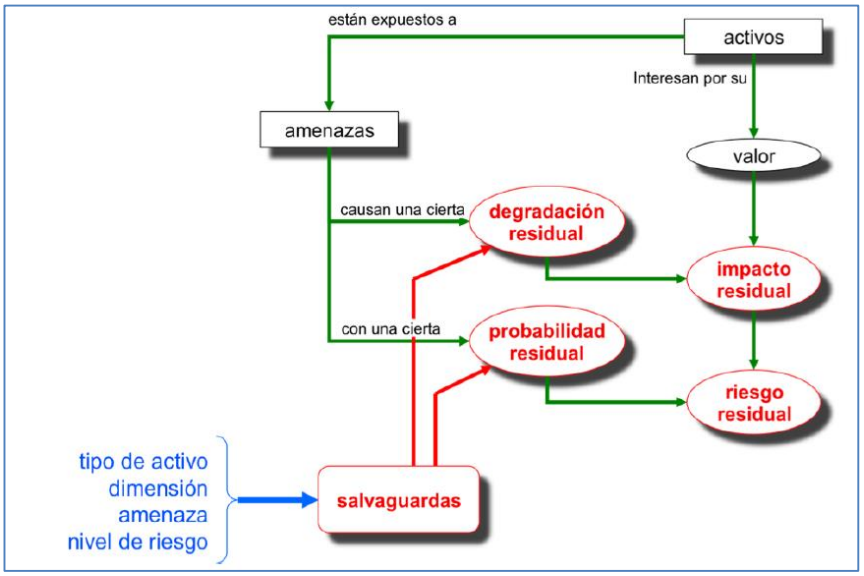
[36] Ibíd., p. 28.

En el Libro III “Guía de técnicas”[37], se pueden encontrar diversos modelos, métricas y escalas en las que se pueden calcular las diferentes variables.

4.1.1.5. Paso 5. Riesgo Residual. Se calcula usando el impacto residual y la probabilidad residual de ocurrencia (es residual en caso de que las salvaguardas afecten la frecuencia de ocurrencia).

La ilustración 3. Muestra como las salvaguardas intervienen directamente disminuyendo la degradación causada por una amenaza y la probabilidad de la misma, dando como resultado el nivel de riesgo residual.

Ilustración 3. Elementos de análisis del riesgo residual



Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, 2012[38].

Proceso de gestión de riesgos. Finalizado el proceso de análisis de riesgos se debe comenzar su gestión, que comprende las actividades del tratamiento del riesgo

[37] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de técnicas. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012.
[38] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro I – Método, Op. cit. p. 32.

residual. Lo primero que se debe realizar es darle una calificación a cada riesgo, como se presenta en el cuadro 17.

Cuadro 17. Estimación del riesgo[39]

Escalas	Riesgo
MA	Crítico
A	Importante
M	Apreciable
B	Bajo
MB	Despreciable

Fuente: Autores.

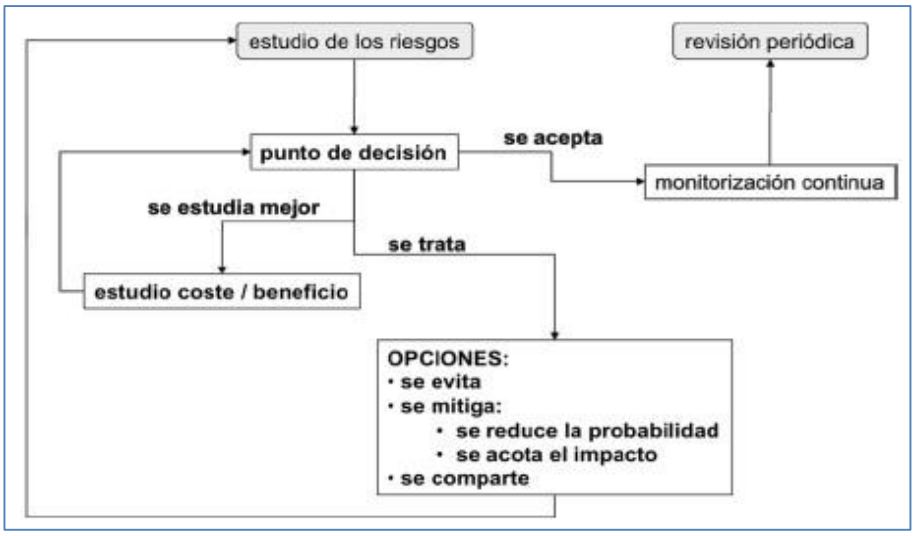
- **Crítico**: Requiere atención inmediatamente.
- **Importante**: Requiere atención, pero es moderada.
- **Apreciable**: Requiere atención.
- **Bajo**: Podría ser objeto de estudio para su tratamiento.
- **Despreciable**: se acepta el riesgo y no se toman acciones al respecto.

La calificación anterior se deriva del impacto o consecuencias que puedan derivar a causa de la materialización de una amenaza, dichas consecuencias por lo general afectan la imagen pública de la organización, indisponibilidad de servicio, pérdidas económicas e implicaciones legales.[40]

La ilustración 4 muestra un esquema de la gestión del riesgo con las actividades y decisiones que se deben realizar una vez se termina el análisis de riesgos, en cierta medida combina en un solo diagrama el proceso de análisis y gestión[41].

[39] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de Técnicas, Op. cit. p. 7.
[40] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro I – Método, Op. cit. p. 47
[41] Ibíd., p. 48.

Ilustración 4. Decisiones de tratamiento de los riesgos



Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, 2012[42].

4.2 MARCO CONCEPTUAL

En general los sistemas de información presentan niveles de seguridad aceptables, sin embargo, las implementaciones de los mismos suelen acarrear ajustes de último momento, usos de plataformas que no están correctamente implementadas y en general una suerte de ajustes de último momento que malogran la seguridad del mismo. Para el caso de la implementación del módulo de Gradebook no se encuentra documentación que detalle el paso a paso que se realizó en el proceso, por lo tanto, es necesario recabar la información de las fuentes humanas que usan y administran el módulo.

En el Planteamiento del Sistema de Gestión de Seguridad de la Información para el Módulo Gradebook se usará como base la norma ISO 27001:2013.

ISO 27001:2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada con base a la norma británica BS 7799-2.

[42] Ibíd., p. 48.

ISO 27001:2013 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001:2013.

Hay 4 ventajas comerciales esenciales que una empresa u organización puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales: cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001:2013 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

- Obtener una ventaja comercial: si una empresa u organización obtiene la certificación y sus competidores no, es posible que la empresa u organización obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

- Menores costos: la filosofía principal de ISO 27001:2013 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos la empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001:2013 es mucho menor que el ahorro que obtendrá.

- Una mejor organización: en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir los procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001:2013 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir los principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de los empleados.[43]

4.3 MARCO HISTORICO

El funcionamiento de la Escuela Colombiana de Carreras Intermedias - ECCI fue autorizado por el Ministerio de Educación Nacional el 25 de octubre de 1978. Inicia la prestación del servicio educativo ofertando los programas de Mecánica

[43] ADVISERA. S.f. ¿Qué es norma ISO 27001? [En línea]. http://advisera.com/27001academy/es/que-es-iso-27001/.

Automotriz, Electromedicina, Química de Plásticos y Electromecánica, debidamente aprobados por la División Académica del ICFES.

A partir de 1980 la ECCI siguió fortaleciéndose académicamente, lo cual le permitió formular nuevos programas del nivel técnico profesional que obtuvieron su registro por parte del entonces Instituto Colombiano para el Fomento de la Educación Superior - ICFES. Estos programas fueron:

- Mecánica Industrial
- Ciencias de la Computación
- Telecomunicaciones
- Desarrollo Ambiental
- Desarrollo Empresarial
- Comercio Exterior
- Gestión Tributaria y Aduanera
- Mercadotecnia
- Diseño de Modas con Enfoque Industrial

En 1994 la ECCI cambió la razón social de la institución a Escuela Colombiana de Carreras Industriales - ECCI, con el fin de seguir ampliando sus horizontes y fortaleciendo su propuesta académica. A partir de 1995 se reciben a técnicos profesionales para que, mediante un plan de transición, continúen sus estudios profesionales de ingeniería, iniciando el proceso a partir del sexto semestre en el primer periodo académico de 1996.

En el año de 1999 la ECCI decidió obtener la acreditación voluntaria de los programas técnicos profesionales, mediante un proceso de mejoramiento continuo, que dio como resultado en los años 2002 y 2003, la obtención de la acreditación de tres de los programas:

- Técnico Profesional en Mecánica Industrial.
- Técnico Profesional en Desarrollo Empresarial.
- Técnico profesional en Electromedicina.

Posteriormente, como consecuencia del proceso de autoevaluación de los programas académicos, la Institución logró la acreditación de siete (7) programas, que se detallan en el cuadro 18.

Cuadro 18. Programas acreditados en alta calidad CNA

Programas en alta calidad	Siglas
Técnico profesional en electromedicina	TPEM
Técnico profesional en tecnología de plásticos	TPTP
Técnico profesional en telecomunicaciones	TPTC
Técnico profesional en electrónica industrial	TPEI
Técnico profesional en comercio exterior y negocios internacionales	TPCEN
Técnico profesional en mecánica automotriz	TPMA
Técnico profesional en desarrollo empresarial	TPDE

Fuente: Oficina de acreditación – ECCI.

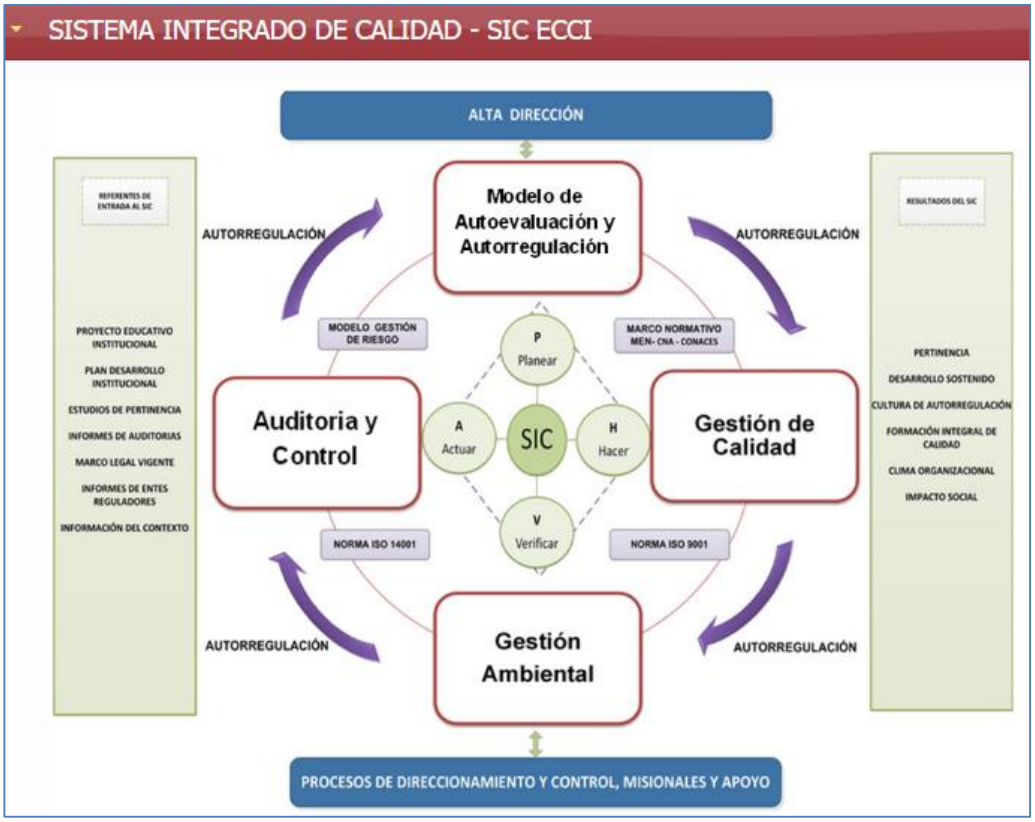
Igualmente, la Institución inició un proceso de reforma estatutaria en el 2002 cambio de carácter académico a Escuela Tecnológica. A partir de este momento la institución inicia la creación de los programas profesionales y de posgrado para ampliar la oferta y expedir las propias titulaciones.

En el año 2004 se firma el convenio entre la Universidad Santiago de Cali – USACA y la Escuela Colombiana de Carreras Industriales – ECCI para llevar programas en extensión a las sedes de la USACA en la ciudad de Palmira y Cali. El proceso se inicia con el programa de Electromedicina y luego se amplía a Mecánica Automotriz, Mecánica Industrial y Desarrollo Empresarial. De igual forma para responder a las necesidades del sector productivo en los diversos campos de la ciencia, la ingeniería, la tecnología y las humanidades con una propuesta académica pertinente, la ECCI amplía su oferta educativa a través de la creación de nuevos programas académicos de pregrado, posgrado y de educación continua, permitiéndole ser reconocida en los sectores educativo y productivo del país.

Es así como la ECCI presenta la documentación pertinente ante el Ministerio de Educación Nacional, para la creación y obtención del registro calificado de las siguientes especializaciones: Automatización Industrial, Producción y Logística Internacional, Telecomunicaciones Inalámbricas, Gerencia de Ingeniería Hospitalaria y Gerencia de Mantenimiento, con el objetivo de brindar a los egresados y demás profesionales la posibilidad de ampliar su formación en un área específica, los cuales cuentan en la actualidad con registro SNIES y registro calificado.

Desde el año 2010 la ECCI cuenta con Certificado en ISO 9001:2008, a continuación en la ilustración 5 se presenta la descripción del Sistema Integrado de Calidad – SIC, por la cual está compuesta la ECCI.

Ilustración 5. Sistema integrado de calidad Universidad ECCI



Fuente: Oficina de calidad Universidad ECCI, S.f[44].

Comité de Calidad: Es el órgano delegado para el desarrollo de las actividades relacionadas con la creación, el diseño, la implementación, mantenimiento y mejoramiento del Sistema de Gestión de la Calidad – SGC de ECCI - Escuela Tecnológica.

[44] UNIVERSIDAD ECCI. S.f. Sistema Integrado de Calidad - SIC [En línea]. <http://bogota.ecci.edu.co/index.php/ecci/sistema-integrado-de-calidad>

Funciones del Comité de Calidad:

Dentro de las funciones más relevantes que tiene el comité se definen:

- Planear, apoyar y asistir el proceso de desarrollo e implementación del SGC de la ECCI.

- Establecer los mecanismos que permitan a los diferentes procesos la aplicación de la política de calidad.

- Elaborar los programas de auditorías internas y evaluar sus resultados.

- Transmitir a la comunidad las políticas de calidad aprobada por la alta dirección en la creación, diseño e implementación de un SGC, orientado a la satisfacción del cliente y el mejoramiento continuo de la Institución.

- Dar adecuado tratamiento a las quejas, reclamos y sugerencias de nuestros clientes internos y externos.

- Estudiar las propuestas de mejora del Sistema de Gestión de la Calidad – SGC producidas por los usuarios internos y externos.

- Velar por el cumplimiento de la Norma Técnica Colombiana NTC ISO 9001:2008.

- Verificar el nivel de cumplimiento de las acciones correctivas, preventivas y de mejora implementadas en el SGC.

- Promover el compromiso de la alta dirección en el desarrollo y mejoramiento del Sistema de Gestión de la Calidad - SGC.

4.4 MARCO LEGAL

La Universidad ECCI – UECCI, cuenta con un sistema de calificación avalado por el Sistema de Aseguramiento de la Calidad de la Educación Superior – SACES donde el docente tiene la autonomía de calificar varias actividades o una por corte, La UECCI tiene estipulado los porcentajes de cada corte que se realiza en la academia para valorar los conocimientos de los estudiantes los cuales se componen

de los siguientes (30% - Primer Corte, 30% - Segundo corte y 40% - tercer corte)[45]. Los docentes no entregan soporte de las notas cargadas en el sistema, aquí se evidencia un riesgo en la integridad de la Información debido a que esta puede ser manipulada después de ser cargada y notificada en el sistema y no existe un soporte impreso o medio magnético de las notas cargas durante el periodo lectivo.

En el mismo sentido la exposición de las notas y en general toda la información del sistema está sujeto a la actual norma de protección de datos 1581 de 2012.

La ley de protección de datos personales "Ley 1581 de 2012" – es una ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

En este sentido se hace preponderante cumplir con el marco legal en Colombia y proteger los diferentes activos de información que hacen parte del módulo gradebook del sistema Académico por la sensibilidad de la información almacenada en el mismo.

4.5 ESTADO ACTUAL

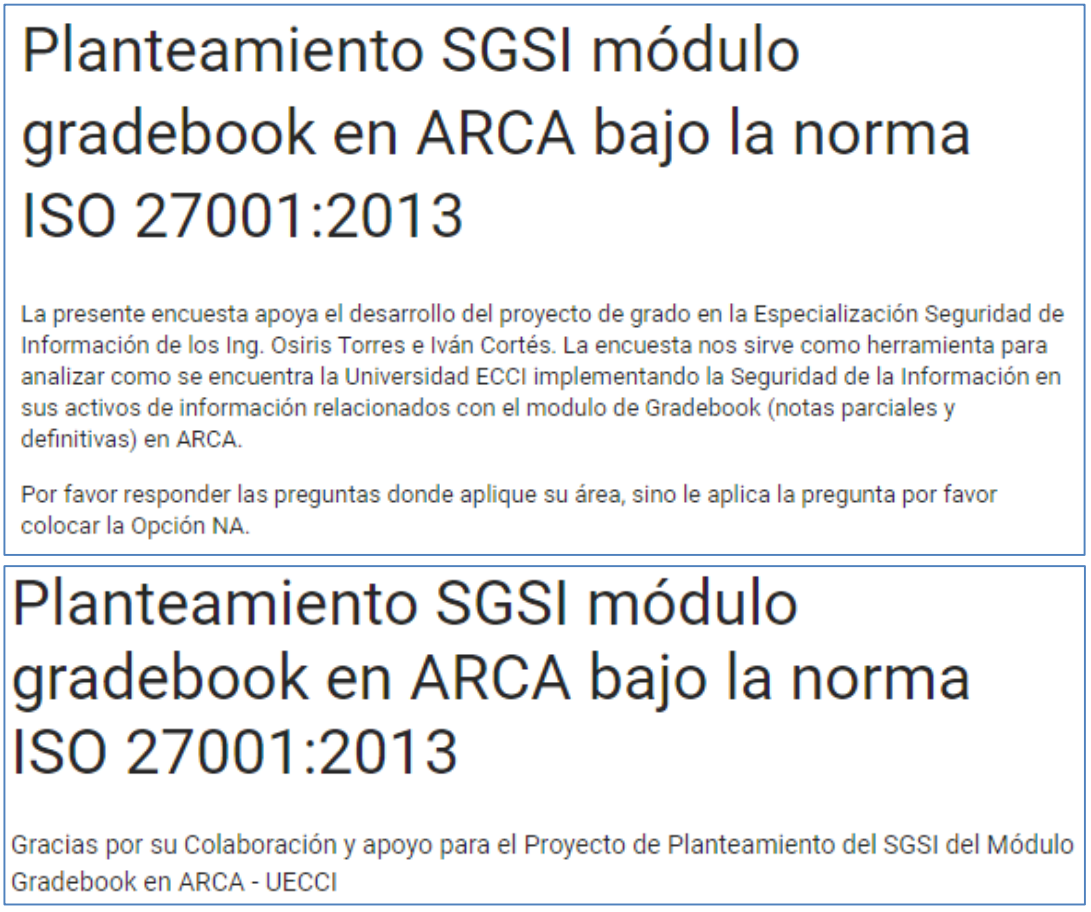
Dentro de las entrevistas realizadas a usuarios administrativos, docentes, estudiantes que tienen relación con el sistema académico y el módulo gradebook, se evidenció que no hay lineamientos o políticas de seguridad de información para el módulo y tampoco para los activos asociados. Se cuenta con el apoyo de la alta dirección para recibir el planteamiento propuesto con fines de implementación y en general los cambios que el desarrollo del proyecto proponga. La Universidad busca fortalecer los procesos que agudicen su actual certificación de calidad ISO 9001:2008 y en general las actividades que permitan fortalecer la plataforma para beneficio de los estudiantes y directivos.

A continuación, se evidencian las entrevistas realizadas al personal que tiene relación con el módulo gradebook en el sistema Académico la cual se desarrolló en torno a cada uno de los controles que se encuentran en el Anexo A, de la Norma ISO 27001:2013.

[45] UNIVERSIDAD ECCI. Artículo 35: Valoración de una asignatura o curso. Op. cit. p. 34.

En la ilustración 6, se presenta la finalidad de la entrevista que se realizó.

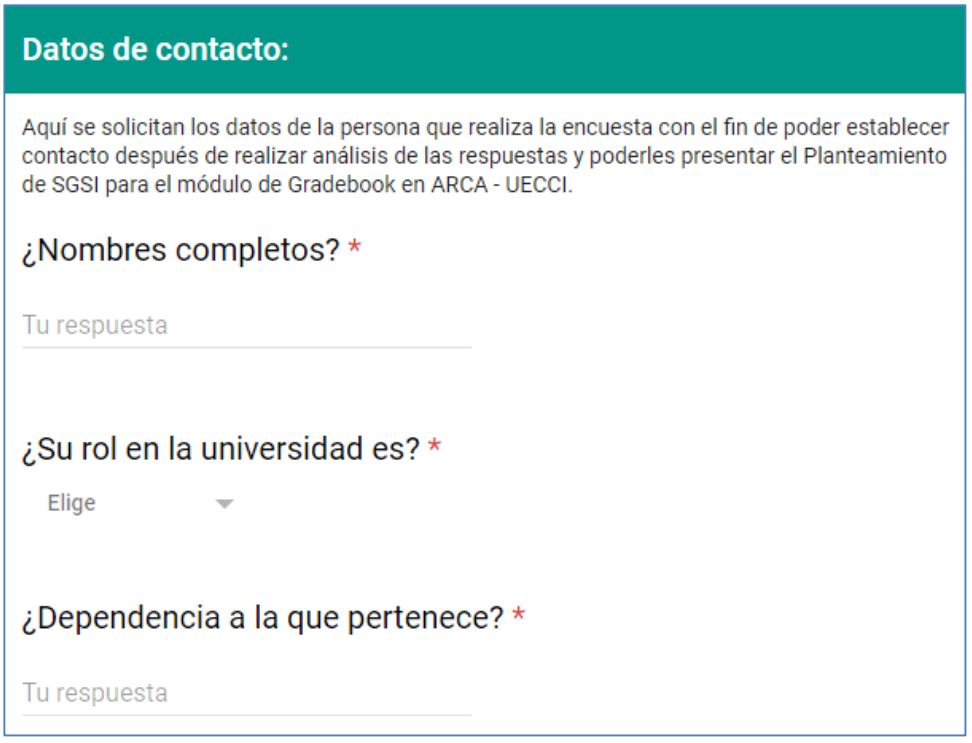
Ilustración 6. Presentación encuesta a usuarios módulo gradebook



Fuente: Autores.

En la ilustración 7, se evidencian los datos que se solicitaron a los usuarios que realizaron la entrevista.

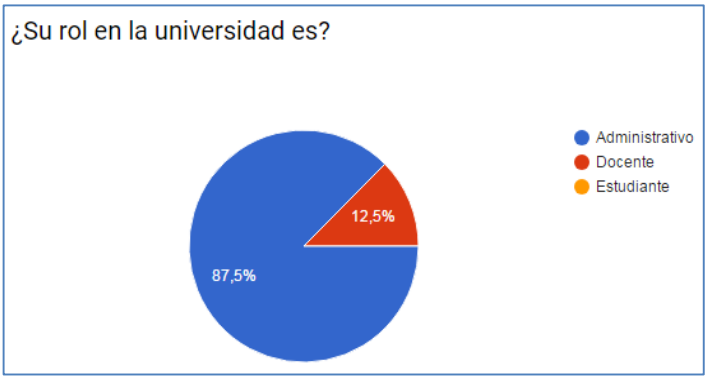
Ilustración 7. Datos de contacto del encuestado



Fuente: Autores.

En la ilustración 8, se identifican los roles de las personas que resolvieron la entrevista.

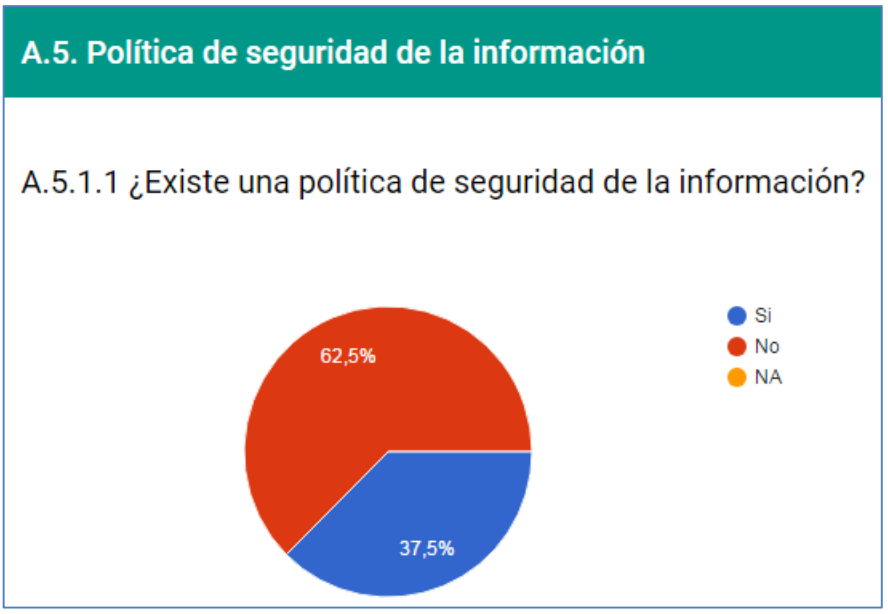
Ilustración 8. Roles que desarrollaron la encuesta



Fuente: Autores.

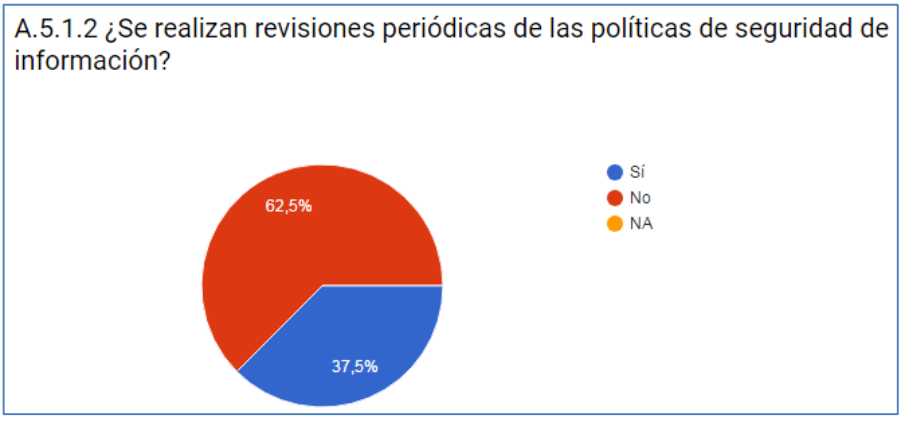
En las ilustraciones 9, 10 y 11 se hacen referencia al control A.5. De la Norma ISO 27001:2013, para conocer si existen políticas establecidas para la seguridad de la Información.

Ilustración 9. Pregunta 1 aplicada



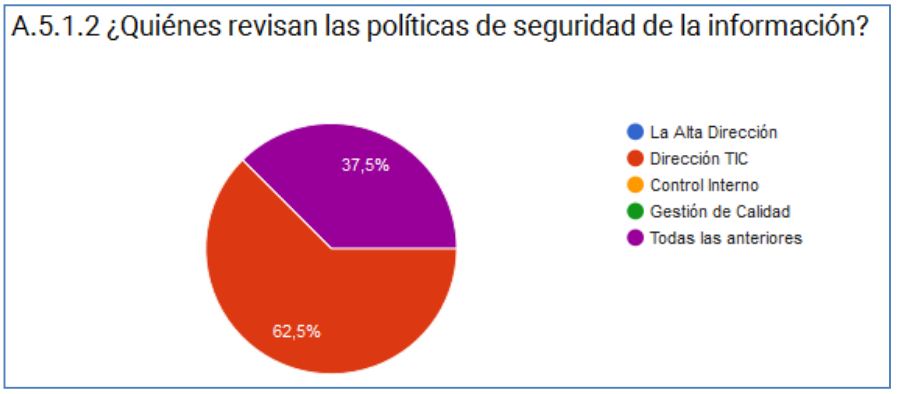
Fuente: Autores.

Ilustración 10. Pregunta 2 aplicada



Fuente: Autores.

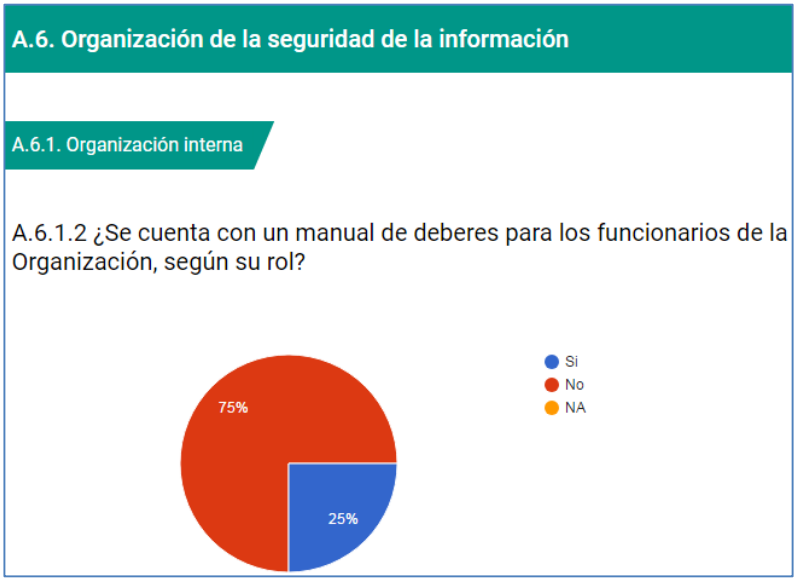
Ilustración 11. Pregunta 3 aplicada



Fuente: Autores.

En la ilustración 12, se evidencia que la UECCI no cuenta con un manual de deberes por roles.

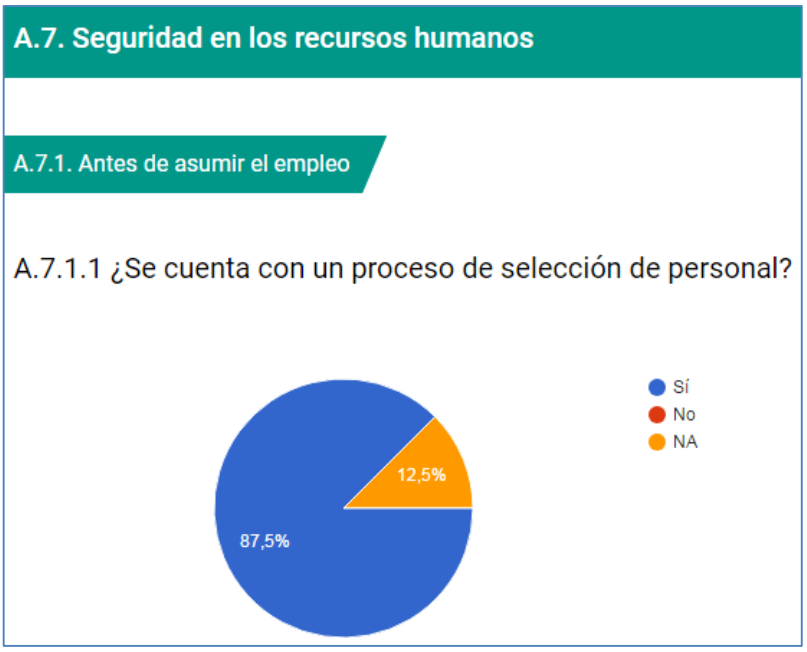
Ilustración 12. Pregunta 4 aplicada



Fuente: Autores.

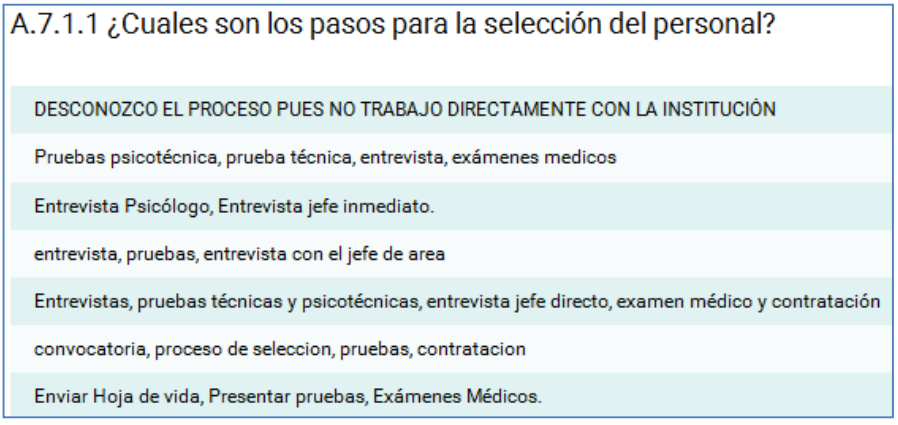
En las ilustraciones 13 y 14 se evalua el control de Seguridad en los Recursos Humanos através del proceso de selección y contratación.

Ilustración 13. Pregunta 5 aplicada



Fuente: Autores.

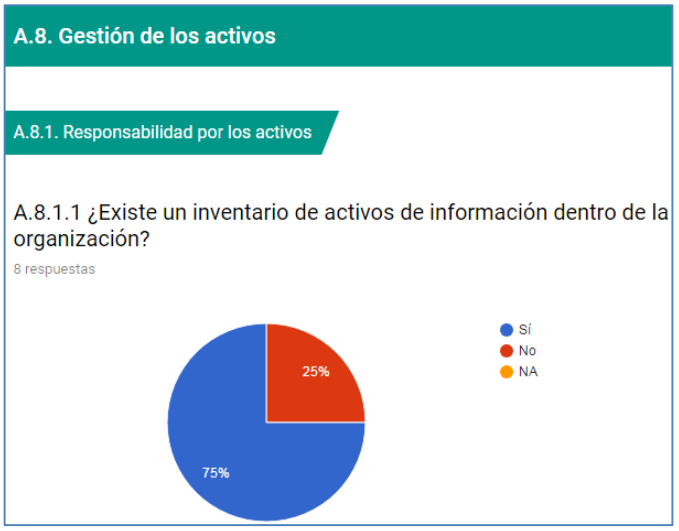
Ilustración 14. Pregunta 6 aplicada



Fuente: Autores.

En la ilustración 15 se evidencia que la mayoría de los usuarios que respondieron la entrevista dicen que si existe un listado de inventario de activos.

Ilustración 15. Pregunta 7 aplicada



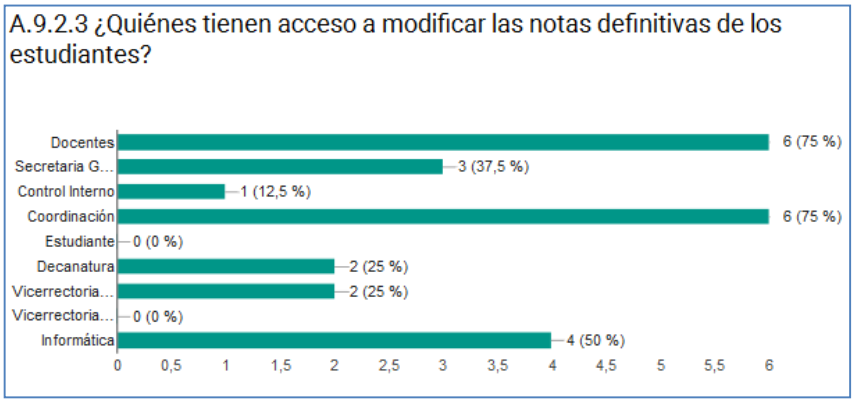
Fuente: Autores.

En la ilustración 16, se muestra que no existe información clara si está estipulada una política de Control de acceso a la UECCI y en la ilustración 17 se identifican quienes tienen acceso a modificar notas.

Ilustración 16. Pregunta 8 aplicada

Fuente: Autores.

Ilustración 17. Pregunta 9 aplicada



Fuente: Autores.

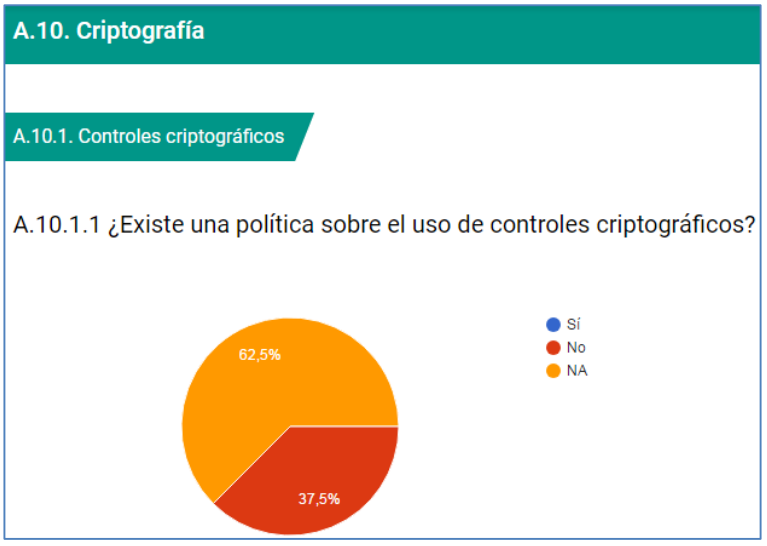
En la ilustración 18, se identifica que no conocen la existencia de la política de gestión de contraseñas.

Ilustración 18. Pregunta 10 aplicada

Fuente: Autores.

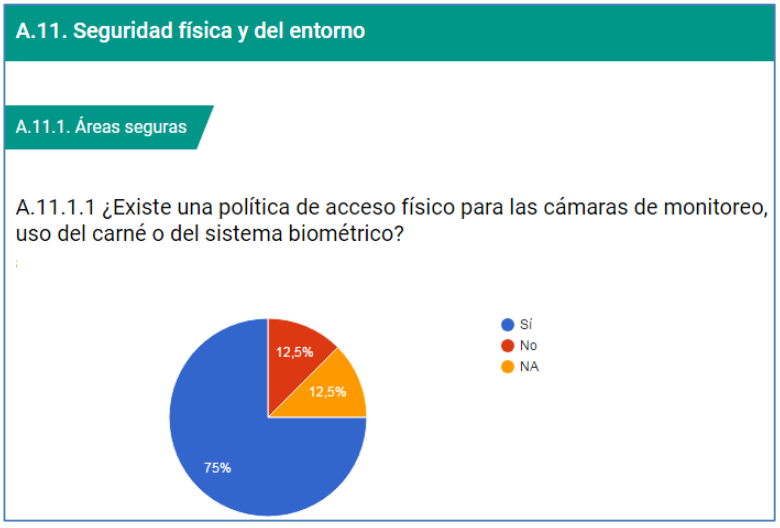
En la ilustración 19, se evidencia que no conocen la política de controles criptográficos y en la ilustración 20, se evidencia claramente que si existe una política de seguridad física y del entorno.

Ilustración 19. Pregunta 11 aplicada



Fuente: Autores.

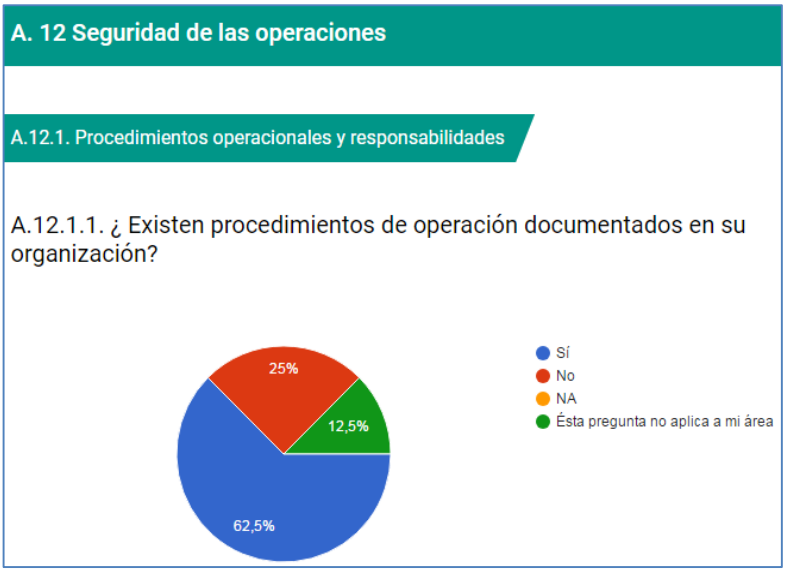
Ilustración 20. Pregunta 12 aplicada



Fuente: Autores.

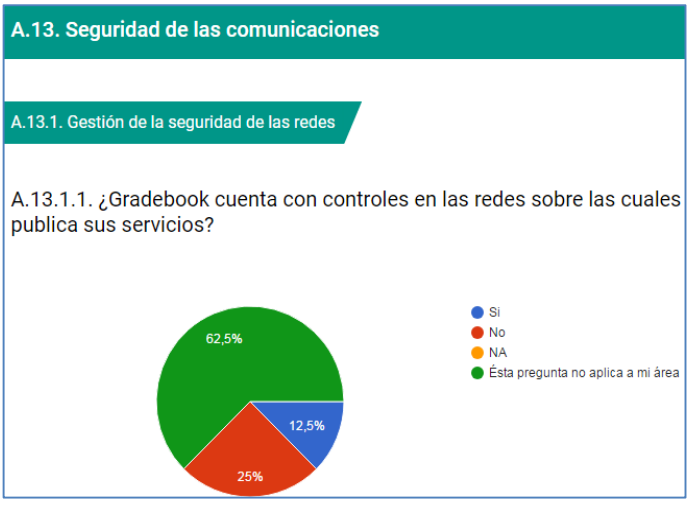
Se evidencia que no hay claridad en los procesos que se ejecutan para la seguridad de las operaciones, ver ilustración 21 y que no se conoce el proceso de los controles aplicados para la seguridad de la red, ver ilustración 22.

Ilustración 21. Pregunta 13 aplicada



Fuente: Autores.

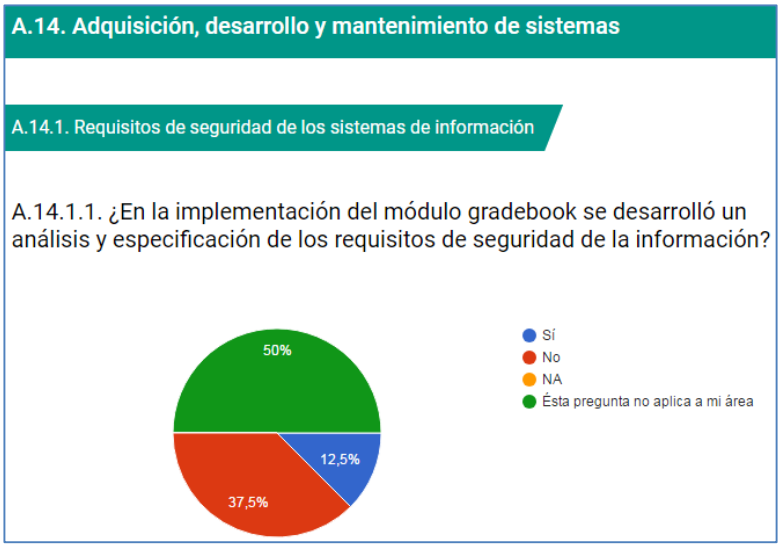
Ilustración 22. Pregunta 14 aplicada



Fuente: Autores.

Debido a la constante rotación de personal del área de Informática encargada del Sistema Académico se ha detectado una falta de conocimiento de los procesos de seguridad con los cuales cuenta la herramienta y este resultado se ve reflejado en las ilustraciones 23 y 24.

Ilustración 23. Pregunta 15 aplicada



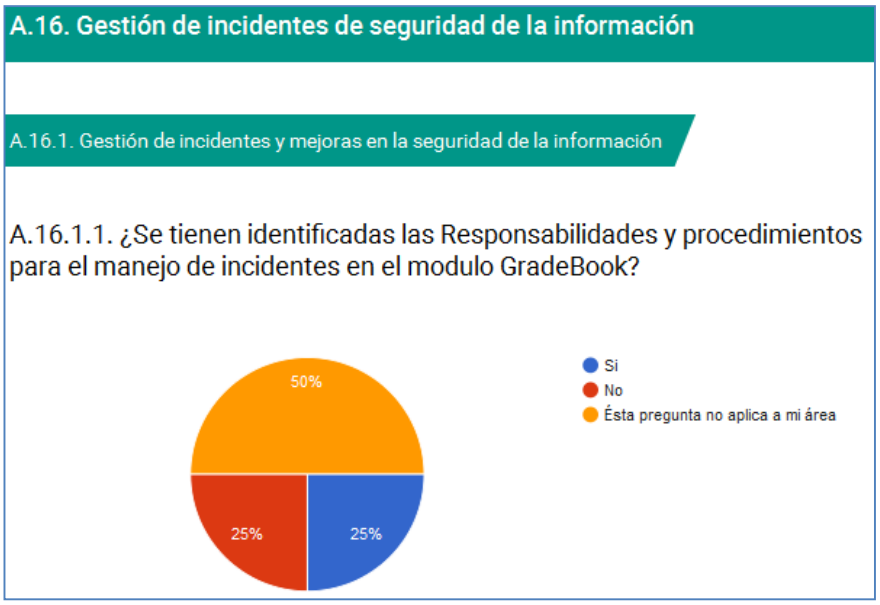
Fuente: Autores

Ilustración 24. Pregunta 16 aplicada

Fuente: Autores.

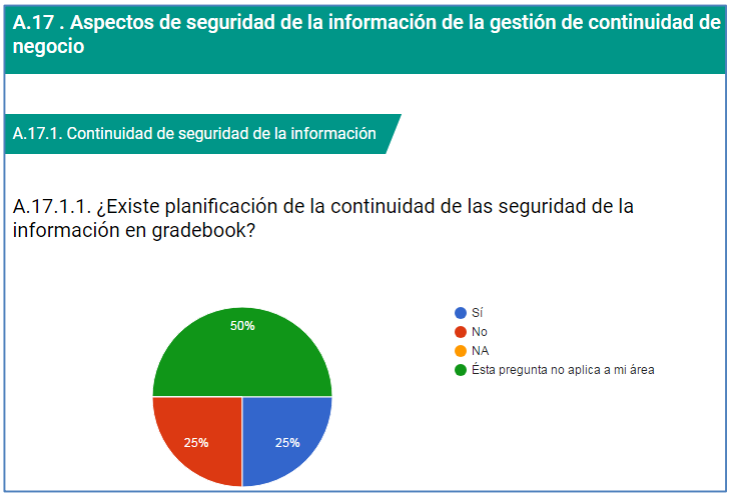
Se evidencia que no estan claras las responsabilidades y los procedimientos al momento de presentarse un incidente en el modulo Gradebook, ver ilustración 25 y no hay se conoce el plan de continuidad para la seguridad del Modulo, ver ilustración 26.

Ilustración 25. Pregunta 17 aplicada



Fuente: Autores.

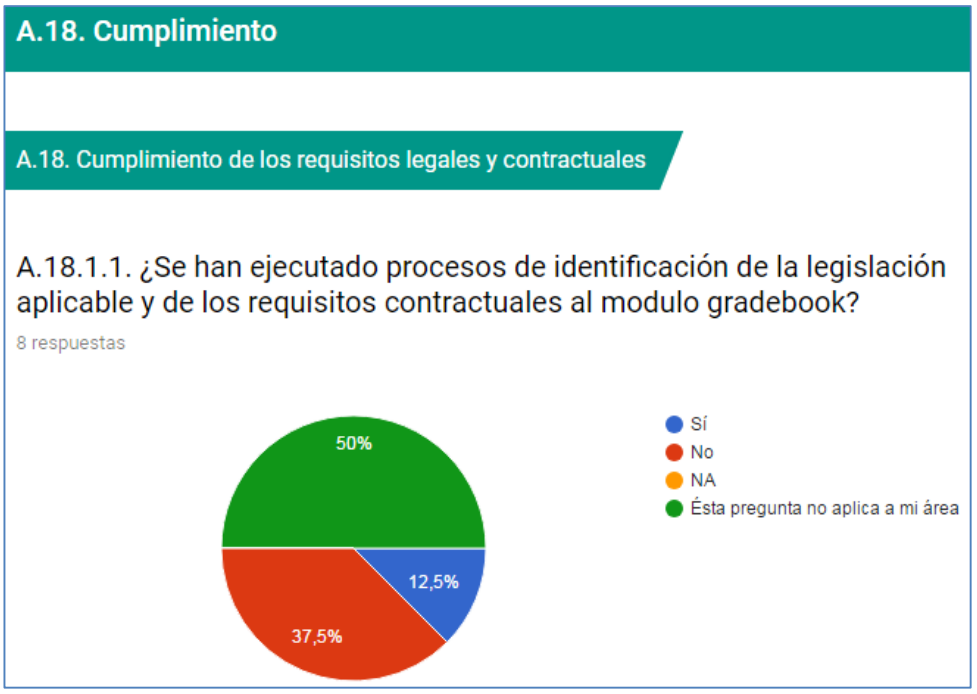
Ilustración 26. Pregunta 18 aplicada



Fuente: Autores.

Se encontró que los usuarios no conocen las leyes que rigen la seguridad de información y las consecuencias que acarea el no cumplirlas, este resultado se ve reflejado en las respuestas que se muestran en la ilustración 27.

Ilustración 27. Pregunta 19 aplicada



Fuente: Autores.

5. DISEÑO METODOLÓGICO

5.1 SELECCIÓN DE METODOLOGÍA

Para el desarrollo del trabajo se ha escogido la metodología de MAGERIT, debido a que cuenta con una estructura organizada para realizar el análisis y gestión de los riesgos enfocados a los sistemas de información y permite el tratamiento de control con la Norma ISO 27001:2013. Esta metodología permite hacer:

- Levantamiento de Activos
- Definición de Amenazas
- Análisis Impacto vs Probabilidad = Riesgo

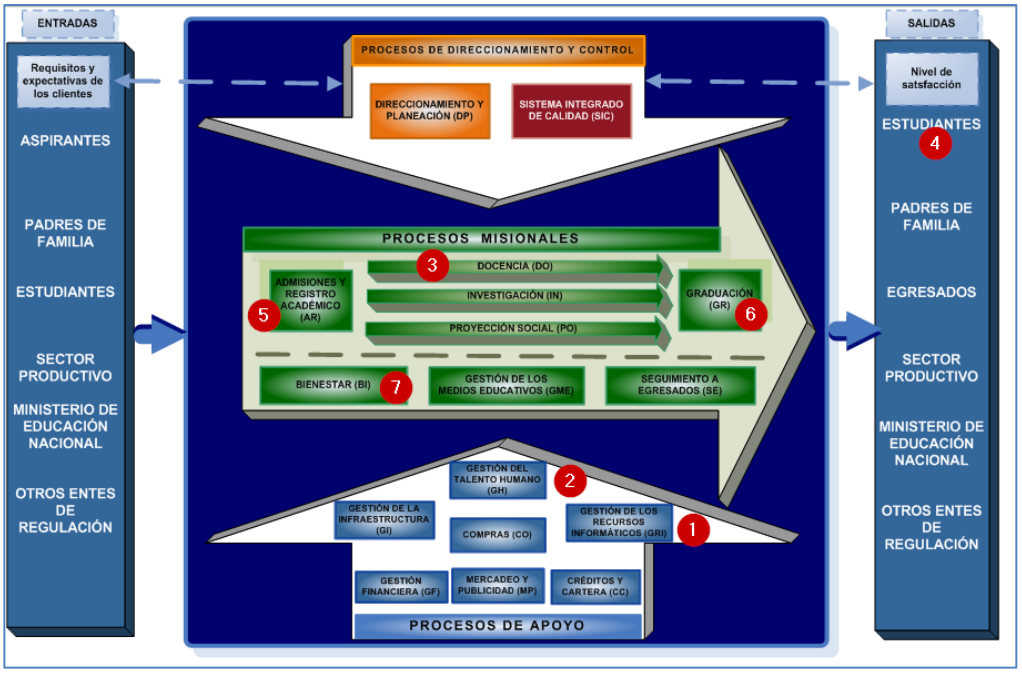
5.2 LEVANTAMIENTO DE ACTIVOS

Dentro del proceso de identificación fue necesario llevar a cabo las siguientes tareas que encaminaron de manera radical el proceso y ayudaron a unificar conceptos para el buen desarrollo del proyecto.

Para poder realizar la identificación de los activos se realizaron las siguientes tareas:

5.2.1 Análisis del mapa de procesos de la Universidad. Identificar en el mapa de procesos, los procesos que están relacionados con el Sistema Académico y en especial con el módulo gradebook como se muestra en la ilustración 28.

Ilustración 28. Mapa de procesos UECCI[46]



Fuente: Autores.

Los procesos involucrados con el Modulo gradebook del Sistema Académico son los siguientes:

- Gestión de los Recursos Informáticos - GRI
- Gestión del talento humano - GH
- Docencia - DO
- Estudiantes- ES
- Admisiones y Registro Académico - AR
- Graduación - GR
- Bienestar – BI

5.2.2 Descripción de los Propietarios y Custodios de los Activos. Ahora se va a describir cada una de las áreas que son propietarias y custodias de los activos de información hallados en cada uno de los procesos anteriormente mencionados que se encuentran relacionados con el módulo Gradebook.

[46] UNIVERSIDAD ECCI. Sistema Integrado de Calidad – SIC, Op. cit. p. 1.

5.2.2.1 Gestión del recurso informático. Es un área de apoyo a la Universidad y está encargada de todo lo referente a lo que abarca una dirección TIC (infraestructura, soporte técnico de equipos y sistemas de Información), en el cuadro 19 se presentan los propietarios y en el cuadro 20 se presentan los custodios de la información que se maneja en ese proceso.

Cuadro 19. Descripción de propietario – GRI

Tipo de proceso	Propietario de la información	Roles
Apoyo	**Gestión de los recursos informáticos**	**Jefe de soporte informático:** verifica, manetiene la Disponibilidad de los equipos de computo esten adecuados para el uso del trabajo de un docente, administrativo, estudiante. **Jefe de informática:** verifica, mantiene la integridad, confidencialidad y disponibilidad de toda la información académica del estudiante tanto en la aplicación como en la Base de Datos. **Jefe de redes:** verifica y mantiene la integridad, confidencialidad y disponibilidad del uso dentro de las sedes de la Universidad. **Jefe de datacenter:** verifica, mantiene la Integridad, Confidencialidad, Disponibilidad de toda la infraestructura tecnologica de la Universidad y de la base de datos del Sistema académico en el cual se encuentra el modulo GradeBook.

Fuente: Autores.

Cuadro 20. Descripción de custodio – GRI

Tipo de proceso	Propietario de la información	Custodio de la información
Apoyo	**Gestión de los recursos informáticos**	Auxiliares de soporte informático Consultores funcionales de informática Auxiliares de redes Auxiliar de datacenter

Fuente: Autores.

5.2.2.2 Gestión del talento humano. En el cuadro 21, se muestran los propietarios de la información que se maneja y en el cuadro 22, se muestran los custodios del proceso de GH.

Cuadro 21. Descripción de propietario – GH

Tipo de proceso	Propietario de la información	Propietarios
Apoyo	**Gestión del talento humano**	**Jefe de gestión humana:** verifica la integridad, confidencialidad de la información del proceso de contratación y culminación del contrato **Auxiliar de selección personal:** verifica la integridad, confidencialidad de la información del proceso de contratación y culminación del contrato

Fuente: Autores.

Cuadro 22. Descripción de custodio – GH

Tipo de proceso	Propietario de la información	Custodio de la información
Apoyo	Gestión del talento humano	Jefe de gestión humana Auxiliar de selección personal

Fuente: Autores.

5.2.2.3 Docencia. En el cuadro 23 se identifica el propietario de las notas y en el cuadro 24 se identifica el custodio de las mismas.

Cuadro 23. Descripción de propietario – DO

Tipo de proceso	Propietario de la información	Roles
Misional	Docencia	Docente: verificar, mantener la integridad, confidencialidad y disponibilidad de las notas Coordinador: verificar, mantener la integridad, confidencialidad y disponibilidad de las notas.

Fuente: Autores.

Cuadro 24. Descripción de custodio – DO

Tipo de proceso	Propietario de la información	Custodio de la información
Misional	**Docencia**	Docente Coordinador

Fuente: Autores.

5.2.2.4 Estudiante. En los cuadros 25 y 26 se evidencia que el propietario y custodio son la misma persona porque nadie más que el estudiante consulta las notas desde su perfil.

Cuadro 25. Descripción de propietario – ES

Tipo de proceso	Propietario de la información	Roles
Salientes	Estudiantes	Estudiante: verifica la integridad y disponibilidad de las notas.

Fuente: Autores.

Cuadro 26. Descripción de custodio – ES

Tipo de proceso	Propietario de la información	Custodio de la información
Salientes	**Estudiantes**	Estudiante

Fuente: Autores.

5.2.2.5 Registro académico. Es el proceso encargado de revisar, verificar que las notas sean las correctas y que siempre estén disponibles para consulta, en el cuadro 27 se identifican los propietarios y en el cuadro 28 se presentan los custodios en este proceso.

Cuadro 27.Descripción de propietario – AR

Tipo de proceso	Propietario de la información	Roles
Misional	Registro académico	Docentes: verificar la integridad, mantener la disponibilidad de las notas. Coordinación: verificar, mantener la integridad, disponibilidad y confidencialidad de las notas. Jefe de secretaria general: verificar, mantener y mejorar la disponibilidad, integridad y confidencialidad de las notas. Jefe de registro y control: mantener la disponibilidad de las notas y su confidencialidad.

Fuente: Autores.

Cuadro 28. Descripción de custodio – AR

Tipo de proceso	Propietario de la información	Custodio de la información
Misional	**Registro académico**	Docente Coordinación Jefe de secretaria general Jefe de registro y control

Fuente: Autores.

5.2.2.6 Graduación. El personal encargado de este proceso son tanto propietarios, ver cuadro 29 como los mismos custodios, ver cuadro 30. Debido que hacen seguimiento al cumplimiento de todo el pensum aprobado.

Cuadro 29. Descripción de propietario – GR

Tipo de proceso	Propietario de la información	Roles
Misional	**Graduación**	**Auxiliares de grados:** verificar la integridad y disponibilidad, mantener la confidencialidad de las notas. **Jede de grados:** verificar la integridad y disponibilidad, mantener la confidencialidad de las notas.

Fuente: Autores.

Cuadro 30. Descripción de custodio – GR

Tipo de proceso	Propietario de la información	Custodio de la información
Misional	**Graduación**	Auxiliares de grados Jefe de grados

Fuente: Autores.

5.2.2.7 Bienestar. Proceso encargado de la mortalidad estudiantil ver los cuadros 31 y 32 para conocer los propietarios y los custodios del proceso.

Cuadro 31. Descripción de propietario – BI

Tipo de proceso	Propietario de la información	Roles
Misional	**Bienestar**	**Jefe de bienestar:** verificar la disponibilidad, mantener la confidencialidad de las notas. **Psicologos de bienestar (proceso de permanencia):** verificar la disponibilidad, mantener la confidencialidad de las notas.

Fuente: Autores.

Cuadro 32. Descripción de custodio – BI

Tipo de proceso	Propietario de la información	Custodio de la información
Misional	**Bienestar**	Jefe de bienestar Psicologos de bienestar (proceso de permanencia)

Fuente: Autores.

5.2.3 Asignación de propietarios y custodios al inventario de activos. Luego de haber identificado los propietarios de cada proceso se procede a asignar propietarios y custodios a cada uno de los activos.

5.2.3.1 Activos asociados al proceso de gestión del recurso informático, ver cuadro 33.

Cuadro 33. Activos de GRI

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A1	Gestión de los recursos informáticos	Equipos de Cómputo Docentes, Administrativos y estudiantes	Distribuidos en áreas administrativas, salas de docentes y salas de sistemas de estudiantes	AHW	En toda la organización	Soporte informático	Auxiliar o técnico de soporte
A2		Licencias de Sistemas Operativos Windows	Distribuidos en áreas administrativas, salas de docentes y salas de sistemas de estudiantes	ASW	Sede C, primer piso - área de soporte informático	Soporte informático	Auxiliar o técnico de soporte
A3		Licencias para Servidores Oracle	Distribuido en el servidor donde se encuentra la base de datos, la aplicación y el los equipos de cómputo asignados a los administradores de la aplicación web y el DBA	ASW	Sede C, primer piso - área de soporte informático	Soporte informático	Auxiliar o técnico de soporte
A4		Sistema de Información PeopleSoft - ARCA (GradeBook)	Distribuida en áreas administrativas y salas de docentes y vía web	ASW	Sede D, 4to. piso en datacenter	Datacenter	Ing. electrónico/ing. sistemas
A5		Manuales de Usuario	Manual que describe toda la navegación que puede realizar un usuario según su rol asignado en gestión humana	AS	Sede C, 1er. piso - área de Informática y vía web	Informática	Auxiliar de informática
A6		Manual de Perfiles en ARCA	Manual que desarrollo el área de Informática para asignar perfiles en el sistema ARCA según las responsabilidades dentro de la organización	AS	Sede C, 1er. piso - área de informática	Informática	Auxiliar de informática
A7		Routers y Switch	Están asignados en varias sedes de la organización	ACOM	En toda la organización	Redes	Técnico de redes
A8		Modem	Están asignados en varias sedes de la organización	ACOM	En toda la organización	Redes	Técnico de redes

Fuente: Autores.

Cuadro 33. Activos de GRI (Continuación)

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A9	Gestión de los recursos informáticos	Cableado UTP	Están asignados en toda la organización	ACOM	En toda la organización	Redes	Técnico de redes
A10		Servidor base de datos ARCA	Servidor donde se encuentra la base de datos del sistema ARCA y el modulo Gradebook	AHW	Sede D, 4to piso en datacenter	Datacenter	Ing. electrónico Ing. sistemas
A11		Servidor de la aplicación web	Servidor donde se encuentra la aplicación web del sistema ARCA y el modulo Gradebook	AHW	Sede D, 4to piso en datacenter	Datacenter	Ing. electrónico Ing. sistemas
A12		Servidor de backups	Servidor donde se encuentra la aplicación web del sistema ARCA y el modulo Gradebook	AHW	Sede D, 4to piso en datacenter	Datacenter	Auxiliar técnico de datacenter
A13		Firewall		ASW	Sede D, 4to piso en datacenter	Datacenter	Ing. electrónico
A14		Rack de datos		AHW	Sede D, 4to piso en datacenter	Datacenter	Auxiliar técnico de datacenter
A15		UPS		AHW	Sede D, 4to piso en datacenter	Datacenter	Auxiliar técnico de datacenter
A16		Bases de datos oracle 11g	Base de datos alimentada por la aplicación web del sistema ARCA, que asignada a los administradores de la aplicación (solo consulta) y al DBA (todos los permisos)	ASW	Sede D, 4to piso en datacenter y área de informática	Datacenter	Especialista en base de datos
A17		Administrador del sistema	Persona que administra el sistema ARCA donde se encuentra el modulo Gradebook	AP	Sede C, Primer Piso área de informática	Datacenter	Especailista en sistemas de información
A18		Administrador de la base de datos	Persona que administra la base de datos de la aplicación ARCA donde se encuentra el modulo Gradebook	AP	Sede D, 4to Piso en datacenter	Datacenter	Especialista en base de datos

Fuente: Autores.

5.2.3.2 Activos asociados al proceso de gestión de talento humano, ver cuadro 34.

Cuadro 34. Activos de GH

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A19	Gestión del talento humano	Seleccionador	Área del talento humano	AP	Sede J, 2do. Piso área de gestión humana	Gestión humana	Auxiliar de selección

Fuente: Autores.

5.2.3.3 Activos asociados al proceso de docencia, ver cuadro 35.

Cuadro 35. Activos de DO

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A20	Docencia	Docente	Persona que asigna la nota parcial y total en el sistema a un estudiante	AP	Dentro y fuera de la organización	Coordinación	Docente

Fuente: Autores.

5.2.3.4 Activos asociados al proceso estudiante, ver cuadro 36.

Cuadro 36. Activos de ES

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A21	Estudiante	Estudiante	Persona que consulta las notas obtenidas en el desarrollo de una materia	AP	Dentro y fuera de la organización	Universidad	Estudiante

Fuente: Autores.

5.2.3.5 Activos asociados al proceso de registro académico, ver cuadro 37.

Cuadro 37. Activos de AR

Información básica del activo						Propiedad del activo	
ID del activo	Proceso	Nombre del activo	Descripción / observaciones	Magerit V3 Tipo_activo	Ubicación	Propietario	Custodio
A22	Registro académico	Registrador	Persona que tiene permisos para modificar notas definitivas culminado un ciclo activo	AP	Sede E, 1er Piso área de admisiones	Secretaria General	Jefe de Registro

Fuente: Autores.

5.3 ANÁLISIS Y GESTIÓN DEL RIESGO BAJO METODOLOGÍA MAGERIT V 3.0

Después de la clara identificación de cada uno de los activos del módulo Gradebook, se procede a realizar el análisis y gestión del riesgo bajo la Metodología MAGERIT.

5.3.1 Amenazas vs activos. Para analizar los activos versus las amenazas se debe tener en cuenta el listado de categorías de amenazas identificado en el marco teórico en capítulo 4.1.1 de este trabajo. A continuación en el cuadro 38, se presentan las amenazas vs cada uno de los activos del inventario.

Cuadro 38. Cruce amenazas vs activos

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM1 - desastres naturales - fuego	X									X	X	X		X	X							
AM2 - desastres naturales - daños por agua	X									X	X	X		X	X							
AM3 - desastres naturales - desastres naturales	X									X	X	X		X	X							
AM4 - de origen industrial - fuego	X									X	X	X		X	X							
AM5 - de origen industrial - daños por agua	X									X	X	X		X	X							
AM6 - de origen industrial - desastres industriales	X									X	X	X		X	X							
AM7 - de origen industrial - contaminación mecánica	X									X	X	X		X	X							
AM8 - de origen industrial - contaminación electromagnética																						
AM9 - de origen industrial - avería de origen físico o lógico	X	X	X	X	X	X				X	X	X	X	X	X							
AM10 - de origen industrial - corte del suministro eléctrico	X									X	X	X		X	X							

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM11 - de origen industrial - condiciones inadecuadas de temperatura o humedad	X									X	X	X		X	X							
AM12 - de origen industrial - fallo de servicios de comunicaciones							X	X	X													
AM13 - de origen industrial - interrupción de otros servicios y suministros esenciales																						
AM14 - de origen industrial - degradación de los soportes de almacenamiento de la información																						
AM15 - de origen industrial - emanaciones electromagnéticas																						
AM16 - errores y fallos no intencionados - errores de los usuarios		X	X	X	X	X							X									
AM17 - errores y fallos no intencionados - errores del administrador	X	X	X	X			X	X	X	X	X	X	X	X	X							
AM18 - errores y fallos no intencionados - errores de monitorización (Log)																						
AM19 - errores y fallos no intencionados - errores de configuración																						
AM20 - errores y fallos no intencionados - deficiencias en la organización	X													X	X		X	X	X	X	X	X

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM21 - errores y fallos no intencionados - difusión de software dañino		X	X	X									X									
AM22 - errores y fallos no intencionados - errores de [re-]encaminamiento		X	X	X			X	X	X				X									
AM23 - errores y fallos no intencionados - errores de secuencia				X			X	X					X									
AM24 - errores y fallos no intencionados - escapes de información					X	X																
AM25 - errores y fallos no intencionados - alteración accidental de la información		X	X	X	X	X	X	X					X									
AM26 - errores y fallos no intencionados - destrucción de información		X	X	X	X	X	X	X					X									
AM27 - errores y fallos no intencionados - fugas de información		X	X	X	X	X	X	X	X				X				X	X	X	X	X	X
AM28 - errores y fallos no intencionados - vulnerabilidades de los programas (software)		X	X	X									X									
AM29 - errores y fallos no intencionados - errores de mantenimiento / actualización de programas (software)		X	X	X	X	X							X									

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM30 - errores y fallos no intencionados - errores de mantenimiento / actualización de equipos (hardware)	X									X	X	X		X	X							
AM31 - errores y fallos no intencionados - caída del sistema por agotamiento de recursos	X						X	X		X	X	X		X	X							
AM32 - errores y fallos no intencionados - pérdida de equipos	X									X	X	X		X	X							
AM33 - errores y fallos no intencionados - indisponibilidad del personal																	X	X	X	X	X	X

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM36 - ataques Intencionados - suplantación de la identidad del usuario		X	X	X	X	X	X	X					X									
AM37 - ataques Intencionados - abuso de privilegios de acceso	X	X	X	X	X	X	X	X		X	X	X	X	X	X							
AM38 - ataques Intencionados - uso no previsto	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							
AM39 - ataques Intencionados - difusión de software dañino		X	X	X									X									
AM40 - ataques Intencionados - [re-]encaminamiento de mensajes				X			X	X	X				X									
AM41 - ataques Intencionados - alteración de secuencia		X	X	X			X	X					X									
AM42 - ataques Intencionados - acceso no autorizado	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																					
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM43 - ataques intencionados - análisis de tráfico							X	X	X													
AM44 - ataques intencionados - repudio																						
AM45 - ataques intencionados - modificación deliberada de la información		X	X	X	X	X	X	X					X									
AM46 - ataques intencionados - destrucción de información		X	X	X	X	X							X									
AM47 - ataques intencionados - divulgación de información		X	X	X	X	X	X	X	X				X									
AM48 - ataques intencionados - manipulación de programas		X	X	X									X									
AM49 - ataques intencionados - manipulación de los equipos	X									X	X	X		X	X							
AM50 - ataques intencionados - denegación de servicio	X						X	X		X	X	X			X							

Fuente: Autores.

Cuadro 38. Cruce amenazas vs activos (Continuación)

	Activos vs amenazas																				
Amenaza / activo	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM51 - ataques intencionados - robo	X									X	X	X		X	X							
AM52 - ataques intencionados - ataque destructivo	X									X	X	X		X	X							
AM53 - ataques intencionados - ocupación enemiga																						
AM54 - ataques intencionados - indisponibilidad del personal																	X	X	X	X	X	X
AM55 - ataques intencionados - extorsión																	X	X	X	X	X	X
AM56 - ataques intencionados - ingeniería social (picaresca)																	X	X	X	X	X	X

Fuente: Autores.

5.3.2 Estimación del riesgo. La gestión del riesgo que se plantea para el módulo de Gradebook (Libro de Notas) en el sistema de Información Académico, es un procedimiento que se usa para valorar cada uno de los activos de información que se relacionan con el módulo a través de la aplicación de la metodología MAGERIT, esta metodología permite identificar los activos, las amenazas que le afecta a cada uno de ellos y cuenta con una escala cualitativa de estimación del riesgo según el impacto y la probabilidad que le aplique a cada activo vs amenaza, en este trabajo se identificaran riesgos ***críticos, importantes, apreciables, bajos y despreciable***[47], en el cuadro 39 se presenta la escala cualitativa de estimación del riesgo con la cual se va a trabajar en el análisis del riesgo:

Cuadro 39. Estimación de Riesgo

Estimación riesgo	
	Crítico
	Importante
	Apreciable
	Bajo
	Despreciable

Fuente: MAGERIT 3.0, 2012[48].

Para calcular el riesgo es necesario realizar la matriz de impacto vs probabilidad. A continuación, se muestra el cuadro 40 la propuesta de MAGERIT y que se implementara en el desarrollo de este proyecto para calcular el riesgo.

[47] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro II – Catalogo de elementos, Op. cit. p. 7.
[48] Ibíd., p. 7.

Cuadro 40. Matriz de impacto * probabilidad = riesgo

Riesgo		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	MA	M	A	A
	B	MB	B	B	MA	M
	MB	MB	MB	MB	B	B

Fuente: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de análisis de riegos, 2012[49].

Se evaluaron los activos versus las amenazas y se obtuvieron los siguientes resultados:

Se evaluaron 56 amenazas (Cap. 4.1.1) por 22 activos que se lograron levantar en el inventario de Activos (Cap. 5.2.3), el cruce de esta información se realizó con ayuda del departamento de calidad, administrativos, docentes y estudiantes, los resultados arrojados han permitido evidenciar que la Universidad no cuenta con un sistema de gestión de seguridad de información para ninguno de los activos encontrados y tampoco se presenta evidencia de políticas de seguridad para el sistema de información académico.

[49] Ibíd., p. 7.

A continuación, se presenta un resumen general de cuantos riesgos se encontraron, ver cuadro 41.

Cuadro 41. Estimación del riesgo (todos los activos ECCI vs amenazas MAGERIT)

Estimación del riesgo					
Impacto / probabilidad	**MB**	**B**	**M**	**A**	**MA**
MA	6	24	53	22	1
A	10	30	59	18	2
M	10	27	20	12	2
B	16	1	1	4	1
MB	2	0	0	0	0
Total de riesgos	**321**				

Fuente: Autores.

Se puede evidenciar que se logró encontrar un total de 321 riesgos que se presentan para el módulo Gradebook, afectando no solo el sistema de información (ASW), el servidor de Base de Datos (AHW), los servicios ofrecidos (AS) y no dejando atrás el personal (Docente, Administrativo, Estudiante), como se puede ver el sistema está compuesto por un todo que tiene varias partes, las cuales sino se protegen el daño de cualquiera de ellas puede afectar el buen funcionamiento del módulo, por ello es importante empezar a plantear políticas de seguridad que permitan mitigar cada uno de estos riesgos en especial los críticos e importantes, pero para el proyecto se trabajaran solo los Críticos (se encontraron 120) y la Universidad asume el trabajo de los importantes (109), apreciables (62), bajo (12) y despreciables (18).

En el cuadro 42, se presentan los riesgos por Activo vs Criticidad, estos resultados permiten verificar cual es el activo que más se está afectando en este momento y que es importante plantear políticas para su óptimo funcionamiento y cuidado.

Cuadro 42. Criticidad riesgo vs tipo_ activo

Riesgo / tipo_activo	Software	Servicio	Personal	Hardware	Comunicaciones
Crítico	49	0	21	34	16
Importante	18	0	12	58	21
Apreciable	17	10	1	27	7
Bajo	0	2	2	7	1
Despreciables	0	16	0	2	0

Fuente: Autores.

Lo que se puede concluir es que los activos más afectados en primer lugar son el Software, El hardware y el personal, todos estos activos son muy importantes para el correcto funcionamiento no solo del módulo Gradebook sino del sistema de información académico, se plantearan políticas y controles para que al momento de implementarlos se pueda mitigar el riesgo y se mejore la seguridad del sistema de información académico, y brindar así Confidencialidad, Disponibilidad e Integridad.

En el análisis del riesgo se encontraron 120 riesgos críticos que son afectados por las diferentes amenazas categorizadas según MAGERIT Cap. (4.1.1).

El impacto de estos riesgos críticos puede causar:

- Interrupción de actividades
- Sanciones por no cumplir con la norma
- Destrucción y perdida de activos relacionados con el módulo Gradebook
- Desventaja Competitiva
- Pérdida de Imagen

A continuación, se especifican los riesgos que se van a tomar para trabajar en esta fase del proyecto, ver cuadro 43.

Cuadro 43. Riesgos críticos a trabajar

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
9	Equipos de Computo Docentes, Administrativos y estudiantes	AM10 - De Origen Industrial - Corte del suministro eléctrico	MA	M	Crítico	AHW
12	Equipos de Computo Docentes, Administrativos y estudiantes	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	A	Crítico	AHW
15	Equipos de Computo Docentes, Administrativos y estudiantes	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	M	Crítico	AHW
16	Equipos de Computo Docentes, Administrativos y estudiantes	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	Crítico	AHW
17	Equipos de Computo Docentes, Administrativos y estudiantes	AM38 - Ataques Intencionados - Uso no previsto	MA	M	Crítico	AHW
21	Equipos de Computo Docentes, Administrativos y estudiantes	AM51 - Ataques Intencionados - Robo	MA	M	Crítico	AHW
26	Licencias de Sistemas Operativos Windows	AM21 - Errores y fallos no intencionados - Difusión de software dañino	MA	M	Crítico	ASW
30	Licencias de Sistemas Operativos Windows	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	ASW
36	Licencias de Sistemas Operativos Windows	dañino	MA	M	Crítico	ASW
37	Licencias de Sistemas Operativos Windows	AM41 - Ataques Intencionados - Alteración de secuencia	MA	M	Crítico	ASW
38	Licencias de Sistemas Operativos Windows	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	Crítico	ASW
39	Licencias de Sistemas Operativos Windows	AM45 - Ataques Intencionados - Modificación deliberada de la información	A	A	Crítico	ASW
40	Licencias de Sistemas Operativos Windows	información	MA	A	Crítico	ASW
41	Licencias de Sistemas Operativos Windows	información	MA	A	Crítico	ASW
42	Licencias de Sistemas Operativos Windows	AM48 - Ataques Intencionados - Manipulación de programas	MA	M	Crítico	ASW
46	Licencias para Servidores Oracle	AM21 - Errores y fallos no intencionados - Difusión de software dañino	MA	M	Crítico	ASW
50	Licencias para Servidores Oracle	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	ASW
56	Licencias para Servidores Oracle	AM39 - Ataques Intencionados - Difusión de software dañino	MA	M	Crítico	ASW
57	Licencias para Servidores Oracle	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	Crítico	ASW

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
58	Licencias para Servidores Oracle	AM42 - Ataques Intencionados - Acceso no autorizado	A	A	Crítico	ASW
59	Licencias para Servidores Oracle	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	B	Crítico	ASW
60	Licencias para Servidores Oracle	AM46 - Ataques Intencionados - Destrucción de información	MA	B	Crítico	ASW
61	Licencias para Servidores Oracle	AM47 - Ataques Intencionados - Divulgación de información	MA	M	Crítico	ASW
62	Licencias para Servidores Oracle	AM48 - Ataques Intencionados - Manipulación de programas	MA	M	Crítico	ASW
63	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM9 - De Origen Industrial - Avería de origen físico o lógico	MA	M	Crítico	ASW
65	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM17 - Errores y fallos no intencionados - Errores del administrador	MA	B	Crítico	ASW
66	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM21 - Errores y fallos no intencionados - Difusión de software dañino	A	A	Crítico	ASW
67	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM22 - Errores y fallos no intencionados - Errores de [re-]encaminamiento	MA	M	Crítico	ASW
68	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM23 - Errores y fallos no intencionados - Errores de secuencia	MA	M	Crítico	ASW
70	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM26 - Errores y fallos no intencionados - Destrucción de información	MA	B	Crítico	ASW
74	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM36 - Ataques Intencionados - Suplantación de la identidad del usuario	MA	M	Crítico	ASW
78	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM40 - Ataques Intencionados - [Re-]encaminamiento de mensajes	MA	M	Crítico	ASW
79	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	Crítico	ASW

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
80	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM42 - Ataques Intencionados - Acceso no autorizado	MA	A	Crítico	ASW
81	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	A	Crítico	ASW
82	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM46 - Ataques Intencionados - Destrucción de información	A	A	Crítico	ASW
113	Routers y Switch	AM12 - De Origen Industrial - Fallo de servicios de comunicaciones	MA	M	Crítico	ACOM
117	Routers y Switch	AM25 - Errores y fallos no intencionados - Alteración accidental de la información	MA	M	Crítico	ACOM
119	Routers y Switch	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	ACOM
122	Routers y Switch	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	A	Crítico	ACOM
123	Routers y Switch	AM38 - Ataques Intencionados - Uso no previsto	MA	M	Crítico	ACOM
127	Routers y Switch	AM43 - Ataques Intencionados - Análisis de tráfico	MA	A	Crítico	ACOM
128	Routers y Switch	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	A	Crítico	ACOM
129	Routers y Switch	AM47 - Ataques Intencionados - Divulgación de información	MA	M	Crítico	ACOM
134	Modem	AM23 - Errores y fallos no intencionados - Errores de secuencia	MA	B	Crítico	ACOM
138	Modem	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	Crítico	ACOM
143	Modem	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	Crítico	ACOM

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
147	Modem	AM47 - Ataques Intencionados - Divulgación de información	MA	B	Crítico	ACOM
149	Cableado UTP	AM12 - De Origen Industrial - Fallo de servicios de comunicaciones	MA	M	Crítico	ACOM
152	Cableado UTP	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	ACOM
155	Cableado UTP	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	Crítico	ACOM
157	Cableado UTP	AM47 - Ataques Intencionados - Divulgación de información	MA	M	Crítico	ACOM
167	Servidor Base de Datos ARCA	AM11 - De Origen Industrial - Condiciones inadecuadas de temperatura o humedad	MA	B	Crítico	AHW
170	Servidor Base de Datos ARCA	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	Crítico	AHW
172	Servidor Base de Datos ARCA	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	A	Crítico	AHW
174	Servidor Base de Datos ARCA	AM42 - Ataques Intencionados - Acceso no autorizado	MA	MA	Crítico	AHW
178	Servidor Base de Datos ARCA	AM52 - Ataques Intencionados - Ataque destructivo	MA	M	Crítico	AHW
188	Servidor de la Aplicación Web	AM11 - De Origen Industrial - Condiciones inadecuadas de temperatura o humedad	MA	B	Crítico	AHW
191	Servidor de la Aplicación Web	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	Crítico	AHW
193	Servidor de la Aplicación Web	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	Crítico	AHW

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
195	Servidor de la Aplicación Web	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	Crítico	AHW
199	Servidor de la Aplicación Web	AM52 - Ataques Intencionados - Ataque destructivo	MA	M	Crítico	AHW
210	Servidor de Backups	AM17 - Errores y fallos no intencionados - Errores del administrador	MA	M	Crítico	AHW
213	Servidor de Backups	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	M	Crítico	AHW
214	Servidor de Backups	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	Crítico	AHW
216	Servidor de Backups	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	Crítico	AHW
220	Servidor de Backups	AM52 - Ataques Intencionados - Ataque destructivo	MA	B	Crítico	AHW
221	Firewall	AM9 - De Origen Industrial - Avería de origen físico o lógico	MA	A	Crítico	ASW
224	Firewall	AM21 - Errores y fallos no intencionados - Difusión de software dañino	MA	A	Crítico	ASW
225	Firewall	AM22 - Errores y fallos no intencionados - Errores de [re-]encaminamiento	A	A	Crítico	ASW
226	Firewall	AM23 - Errores y fallos no intencionados - Errores de secuencia	A	A	Crítico	ASW
227	Firewall	AM25 - Errores y fallos no intencionados - Alteración accidental de la información	MA	A	Crítico	ASW
228	Firewall	AM26 - Errores y fallos no intencionados - Destrucción de información	MA	A	Crítico	ASW
229	Firewall	AM27 - Errores y fallos no intencionados - Fugas de información	MA	A	Crítico	ASW

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
230	Firewall	AM28 - Errores y fallos no intencionados - Vulnerabilidades de los programas (software)	A	A	Crítico	ASW
232	Firewall	AM36 - Ataques Intencionados - Suplantación de la identidad del usuario	MA	A	Crítico	ASW
233	Firewall	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	A	Crítico	ASW
234	Firewall	AM38 - Ataques Intencionados - Uso no previsto	A	A	Crítico	ASW
235	Firewall	AM39 - Ataques Intencionados - Difusión de software dañino	MA	A	Crítico	ASW
236	Firewall	AM40 - Ataques Intencionados - [Re-]encaminamiento de mensajes	A	A	Crítico	ASW
237	Firewall	AM41 - Ataques Intencionados - Alteración de secuencia	A	A	Crítico	ASW
238	Firewall	AM42 - Ataques Intencionados - Acceso no autorizado	MA	A	Crítico	ASW
239	Firewall	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	A	Crítico	ASW
240	Firewall	AM46 - Ataques Intencionados - Destrucción de información	MA	A	Crítico	ASW
241	Firewall	AM47 - Ataques Intencionados - Divulgación de información	MA	A	Crítico	ASW
242	Firewall	AM48 - Ataques Intencionados - Manipulación de programas	A	A	Crítico	ASW
243	Rack de Datos	AM1 - Desastres Naturales - Fuego	MA	B	Crítico	AHW
244	Rack de Datos	AM2 - Desastres Naturales - Daños por agua	MA	B	Crítico	AHW

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
245	Rack de Datos	AM3 - Desastres Naturales - Desastres naturales	MA	B	Crítico	AHW
246	Rack de Datos	AM4 - De Origen Industrial - Fuego	MA	B	Crítico	AHW
247	Rack de Datos	AM5 - De Origen Industrial - Daños por agua	MA	B	Crítico	AHW
248	Rack de Datos	AM6 - De Origen Industrial - Desastres industriales	MA	B	Crítico	AHW
250	Rack de Datos	AM9 - De Origen Industrial - Avería de origen físico o lógico	A	A	Crítico	AHW
251	Rack de Datos	AM10 - De Origen Industrial - Corte del suministro eléctrico	MA	M	Crítico	AHW
252	Rack de Datos	AM11 - De Origen Industrial - Condiciones inadecuadas de temperatura o humedad	MA	M	Crítico	AHW
254	Rack de Datos	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	M	Crítico	AHW
257	Rack de Datos	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	B	Crítico	AHW
260	Rack de Datos	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	Crítico	AHW
263	Rack de Datos	AM52 - Ataques Intencionados - Ataque destructivo	MA	M	Crítico	AHW
287	Administrador del Sistema	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	AP
288	Administrador del Sistema	AM33 - Errores y fallos no intencionados - Indisponibilidad del personal	MA	M	Crítico	AP
289	Administrador del Sistema	AM54 - Ataques Intencionados - Indisponibilidad del personal	MA	M	Crítico	AP

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
290	Administrador del Sistema	AM55 - Ataques Intencionados - Extorsión	MA	B	Crítico	AP
291	Administrador del Sistema	AM56 - Ataques Intencionados - Ingeniería social (picaresca)	A	MA	Crítico	AP
293	Administrador de la Base de Datos	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	AP
294	Administrador de la Base de Datos	AM33 - Errores y fallos no intencionados - Indisponibilidad del personal	MA	M	Crítico	AP
295	Administrador de la Base de Datos	AM54 - Ataques Intencionados - Indisponibilidad del personal	MA	M	Crítico	AP
296	Administrador de la Base de Datos	AM55 - Ataques Intencionados - Extorsión	MA	B	Crítico	AP
297	Administrador de la Base de Datos	AM56 - Ataques Intencionados - Ingeniería social (picaresca)	A	MA	Crítico	AP
298	Selección y contratación (Docentes, administrativos)	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	A	Crítico	AP
299	Selección y contratación (Docentes, administrativos)	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	AP
302	Selección y contratación (Docentes, administrativos)	AM55 - Ataques Intencionados - Extorsión	MA	B	Crítico	AP
303	Selección y contratación (Docentes, administrativos)	AM56 - Ataques Intencionados - Ingeniería social (picaresca)	A	A	Crítico	AP
308	Persona que actua e interactua dentro del sistema y la Organización (docente)	AM55 - Ataques Intencionados - Extorsión	A	A	Crítico	AP
314	Persona que actua e interactua dentro del sistemay la Organización (estudiante)	AM55 - Ataques Intencionados - Extorsión	A	A	Crítico	AP
316	Persona que actua e interactua dentro del sistemay la Organización (registro Academico)	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	M	Crítico	AP
317	Persona que actua e interactua dentro del sistemay la Organización (registro Academico)	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	Crítico	AP

Fuente: Autores.

Cuadro 43. Riesgos críticos a trabajar (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación de riesgo	Tipo de activo
318	Persona que actua e interactua dentro del sistemay la Organización (registro Academico)	AM33 - Errores y fallos no intencionados - Indisponibilidad del personal	MA	B	Crítico	AP
319	Persona que actua e interactua dentro del sistemay la Organización (registro Academico)	AM54 - Ataques Intencionados - Indisponibilidad del personal	MA	B	Crítico	AP
320	Persona que actua e interactua dentro del sistemay la Organización (registro Academico)	AM55 - Ataques Intencionados - Extorsión	MA	M	Crítico	AP

Fuente: Autores.

En el cuadro 44, se presentan los riesgos críticos encontrados que afectan el hardware.

Cuadro 44. Amenazas asociadas al hardware

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
9	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM10 - De Origen Industrial - Corte del suministro eléctrico	MA	M	**Crítico**	**AHW**
12	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	A	**Crítico**	**AHW**
15	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	M	**Crítico**	**AHW**
16	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	**Crítico**	**AHW**
17	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM38 - Ataques Intencionados - Uso no previsto	MA	M	**Crítico**	**AHW**
21	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM51 - Ataques Intencionados - Robo	MA	M	**Crítico**	**AHW**

Fuente: Autores.

Cuadro 44. Amenazas asociadas al hardware (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
167	Servidor Base de Datos ARCA	AM11 - De Origen Industrial - Condiciones inadecuadas de temperatura o humedad	MA	B	**Crítico**	**AHW**
170	Servidor Base de Datos ARCA	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	**Crítico**	**AHW**
172	Servidor Base de Datos ARCA	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	A	**Crítico**	**AHW**
174	Servidor Base de Datos ARCA	AM42 - Ataques Intencionados - Acceso no autorizado	MA	MA	**Crítico**	**AHW**
178	Servidor Base de Datos ARCA	AM52 - Ataques Intencionados - Ataque destructivo	MA	M	**Crítico**	**AHW**
188	Servidor de la Aplicación Web	AM11 - De Origen Industrial - Condiciones inadecuadas de temperatura o humedad	MA	B	**Crítico**	**AHW**
191	Servidor de la Aplicación Web	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	**Crítico**	**AHW**
193	Servidor de la Aplicación Web	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	**Crítico**	**AHW**

Fuente: Autores.

Análisis:

- Aunque se cuenta con personal para realizar el mantenimiento del hardware de tipo preventivo, correctivo y predictivo en los diferentes equipos de cómputo no se cumple con el cronograma de mantenimiento propuesto a inicio del año lectivo debido a las fechas de terminación del contrato.

- No se cuenta con una base de conocimiento de los casos que se pueden presentar para incidencia en los equipos de cómputo, por lo tanto, cada técnico de soporte resuelve el servicio de forma distinta según su experiencia y conocimiento, en ocasiones la solución puede ser exitosa pero no la más eficiente y la más eficaz, por lo tanto se debe crear una base de conocimiento donde se documenten las incidencias para poder normalizar todos los procesos técnicos.

- No se cuenta con restricciones para dispositivos de almacenamiento USB, aunque se cuenta con un sistema de protección contra virus para mitigar los riesgos de contagio de virus, las unidades de almacenamiento de USB pueden fácilmente afectar a un Sistema de Información.

En el cuadro 45, se presentan los riesgos críticos encontrados que afectan el software.

Cuadro 45. Amenazas asociadas al software

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
26	Licencias de Sistemas Operativos Windows	AM21 - Errores y fallos no intencionados - Difusión de software dañino	MA	M	**Crítico**	**ASW**
30	Licencias de Sistemas Operativos Windows	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	**Crítico**	**ASW**
36	Licencias de Sistemas Operativos Windows	AM39 - Ataques Intencionados - Difusión de software dañino	MA	M	**Crítico**	**ASW**
37	Licencias de Sistemas Operativos Windows	AM41 - Ataques Intencionados - Alteración de secuencia	MA	M	**Crítico**	**ASW**
38	Licencias de Sistemas Operativos Windows	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	**Crítico**	**ASW**
39	Licencias de Sistemas Operativos Windows	AM45 - Ataques Intencionados - Modificación deliberada de la información	A	A	**Crítico**	**ASW**

Fuente: Autores.

Cuadro 45. Amenazas asociadas al software (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
40	Licencias de Sistemas Operativos Windows	AM46 - Ataques Intencionados - Destrucción de información	MA	A	**Crítico**	**ASW**
41	Licencias de Sistemas Operativos Windows	AM47 - Ataques Intencionados - Divulgación de información	MA	A	**Crítico**	**ASW**
42	Licencias de Sistemas Operativos Windows	AM48 - Ataques Intencionados - Manipulación de programas	MA	M	**Crítico**	**ASW**
46	Licencias para Servidores Oracle	AM21 - Errores y fallos no intencionados - Difusión de software dañino	MA	M	**Crítico**	**ASW**
50	Licencias para Servidores Oracle	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	**Crítico**	**ASW**
56	Licencias para Servidores Oracle	AM39 - Ataques Intencionados - Difusión de software dañino	MA	M	**Crítico**	**ASW**
57	Licencias para Servidores Oracle	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	**Crítico**	**ASW**

Fuente: Autores.

Cuadro 45. Amenazas asociadas al software (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
59	Licencias para Servidores Oracle	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	B	**Crítico**	**ASW**
60	Licencias para Servidores Oracle	AM46 - Ataques Intencionados - Destrucción de información	MA	B	**Crítico**	**ASW**
61	Licencias para Servidores Oracle	AM47 - Ataques Intencionados - Divulgación de información	MA	M	**Crítico**	**ASW**
62	Licencias para Servidores Oracle	AM48 - Ataques Intencionados - Manipulación de programas	MA	M	**Crítico**	**ASW**
63	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM9 - De Origen Industrial - Avería de origen físico o lógico	MA	M	**Crítico**	**ASW**
65	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM17 - Errores y fallos no intencionados - Errores del administrador	MA	B	**Crítico**	**ASW**

Fuente: Autores.

Cuadro 45. Amenazas asociadas al software (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
66	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM21 - Errores y fallos no intencionados - Difusión de software dañino	A	A	**Crítico**	**ASW**
67	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM22 - Errores y fallos no intencionados - Errores de [re-]encaminamiento	MA	M	**Crítico**	**ASW**
68	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM23 - Errores y fallos no intencionados - Errores de secuencia	MA	M	**Crítico**	**ASW**
70	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM26 - Errores y fallos no intencionados - Destrucción de información	MA	B	**Crítico**	**ASW**
74	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM36 - Ataques Intencionados - Suplantación de la identidad del usuario	MA	M	**Crítico**	**ASW**
78	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM40 - Ataques Intencionados - [Re-]encaminamiento de mensajes	MA	M	**Crítico**	**ASW**
79	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	**Crítico**	**ASW**

Fuente: Autores.

Cuadro 45. Amenazas asociadas al software (Continuación)

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
80	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM42 - Ataques Intencionados - Acceso no autorizado	MA	A	**Crítico**	**ASW**
81	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	A	**Crítico**	**ASW**
82	Sistema de Información PeopleSoft - ARCA (GradeBook)	AM46 - Ataques Intencionados - Destrucción de información	A	A	**Crítico**	**ASW**

Fuente: Autores.

Análisis:

- La Universidad cuenta con licencias legales gracias a la compra de licencias perpetuas o renovaciones anuales para sus equipos de cómputo, los desarrollos que se realicen dentro de la institución están licenciados sin embargo se evidencia un gran problema y es que no se cuenta con un control para la instalación de software ilegal, o la debida autorización del personal de Soporte Informático.

- No se cuenta con un plan de tratamiento para la baja de equipos, cuando se actualizan o se cambian, solo se realiza formateo para entregar al siguiente usuario si el equipo sigue en uso, se saca un backup de la información privada de las máquinas y se sube a la nube, pero no se cuenta con una política de seguridad de la información que reposa en la nube.

- No se cuenta con un procedimiento para la actualización de parches de seguridad o software en los sistemas críticos de la Universidad.

- En el Firewall se presentan cuellos de botella debido a que hoy en día se está manejando la virtualización de computadores, para mitigar este riesgo se recomienda mejorar equipos de comunicación.

- Existen reglas de protección de acceso a los firewalls desde la red externa a servicios y servidores específicos en la red de servidores DMZ (Desmilitarizada), sin embargo, se evidencia que en la red inalámbrica se puede tener acceso a través de los puertos abiertos a servicios restringidos y esto representa una fuente de riesgo latente y de poner mucho cuidado.

En el cuadro 46, se muestran los riesgos críticos que afectan las redes de comunicación.

Cuadro 46. Amenazas asociadas a las redes de comunicación

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
113	Routers y Switch	AM12 - De Origen Industrial - Fallo de servicios de comunicaciones	MA	M	**Crítico**	**ACOM**
117	Routers y Switch	AM25 - Errores y fallos no intencionados - Alteración accidental de la información	MA	M	**Crítico**	**ACOM**
119	Routers y Switch	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	**Crítico**	**ACOM**
122	Routers y Switch	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	A	**Crítico**	**ACOM**
123	Routers y Switch	AM38 - Ataques Intencionados - Uso no previsto	MA	M	**Crítico**	**ACOM**
127	Routers y Switch	AM43 - Ataques Intencionados - Análisis de tráfico	MA	A	**Crítico**	**ACOM**
128	Routers y Switch	AM45 - Ataques Intencionados - Modificación deliberada de la información	MA	A	**Crítico**	**ACOM**

Fuente: Autores.

Análisis:

- La red se encuentra segmentada física y lógicamente en la totalidad de la Institución, lo cual además de ayudar a mejorar la seguridad de la red mejora el rendimiento y trafico innecesario, sin embargo se manejan subredes y en estas los usuarios hacen daños que son complejos para mitigar, debido a que la configuración no se aplica tan al detalle como la red principal.

- Los sistemas de protección perimetral que posee la institución se ven amenazados debido a que se realizan actualizaciones de seguridad a través de copias, pero estas copias de seguridad se encuentran en un solo punto que es el datacenter, se recomienda guardar copia en otra parte de la institución, sede o si es el caso en la nube para que no se afecte el correcto funcionamiento de los sistemas en caso de ocurrir un desastre industrial en el datacenter.

- Las redes de cada sede de la Institución son diferentes a nivel de direccionamiento y los enlaces a servicios o servidores son administrados por medio de mapeo interno de direcciones entre los firewall y VLANs en los switch, sin embargo se evidencia que el mapeo de estas redes cuenta con dos copias una en servidor y otra en físico pero ambos se encuentran en el mismo sitio, en caso de ocurrir un desastre industrial o natural puede haber perdida de esta información y afectar el buen funcionamiento de la red. Se recomienda contar con una copia del mapeo en un sitio fuera de la institución para consultas en caso de pérdida de la información que se encuentra en el datacenter.

En el cuadro 47, se muestran los riesgos críticos que afectan el activo relacionado con personal.

Cuadro 47. Amenazas asociadas al personal

Numero de riesgo	Activo	Amenaza	Impacto	Probabilidad	Clasificación del riesgo	Tipo de activo
129	Routers y Switch	AM47 - Ataques Intencionados - Divulgación de información	MA	M	**Crítico**	**ACOM**
134	Modem	AM23 - Errores y fallos no intencionados - Errores de secuencia	MA	B	**Crítico**	**ACOM**
138	Modem	AM31 - Errores y fallos no intencionados - Caída del sistema por agotamiento de recursos	A	A	**Crítico**	**ACOM**
143	Modem	AM41 - Ataques Intencionados - Alteración de secuencia	MA	B	**Crítico**	**ACOM**
147	Modem	AM47 - Ataques Intencionados - Divulgación de información	MA	B	**Crítico**	**ACOM**
149	Cableado UTP	AM12 - De Origen Industrial - Fallo de servicios de comunicaciones	MA	M	**Crítico**	**ACOM**
152	Cableado UTP	AM27 - Errores y fallos no intencionados - Fugas de información	MA	M	**Crítico**	**ACOM**
155	Cableado UTP	AM42 - Ataques Intencionados - Acceso no autorizado	MA	M	**Crítico**	**ACOM**
157	Cableado UTP	AM47 - Ataques Intencionados - Divulgación de información	MA	M	**Crítico**	**ACOM**

Fuentes: Autores.

Análisis:

- En la Institución se evidencia un proceso de selección de docente en la cual la coordinación presenta el requerimiento a talento humano, en talento humano envían la convocatoria a través de diferentes medios y cuando ya hay personas optando por la vacante se envían a la coordinación para que realicen las pruebas técnicas y la coordinación lleva con comunicado para radicar a talento humano junto con un formato de los resultados obtenidos por cada aspirante al cargo de docente y ellos culminan el proceso de selección a través de los exámenes médicos y pruebas psicotécnicas, lo que se evidencia aquí es que el proceso de contratación es demorado y afecta el correcto funcionamiento de las labores que debe realizar un docente dentro del sistema académico por falta de tiempo para brindar la capacitación, entre esas el registro de notas a tiempo en el sistema académico, no solo se ve afectado el docente por el cierre de plazo para cargar notas en el sistema sino que se ve afectado el estudiante debido a que no se le publican sus notas parciales a tiempo en el sistema de información académico. Se recomienda que la contratación docente se haga con un tiempo prudencial antes de iniciar el ciclo lectivo, así el docente ingresa a la institución con tiempo y se puede capacitar para así evitar que manipule el sistema con desconocimiento y cometa errores no intencionados.

6. PLANTEAMIENTO DE LOS CONTROLES QUE SE DEBEN APLICAR BAJO LA NORMA ISO 27001:2013 A LOS RIESGOS ENCONTRADOS EN EL ANÁLISIS

En el siguiente aparte se encuentra relacionado cada uno de los controles que se plantean aplicar en cada uno de los riesgos críticos trabajados en el proyecto. Se encuentra cada activo con su amenaza y el control que puede aplicar bajo la norma ISO 27001:2013, toda esta información se puede visualizar desde el cuadro 48-63.

Cuadro 48.Activo 1 vs controles ISO 27001:2013

A1 - Equipos de computo docentes, administrativos y estudiantes	
Amenazas	**Norma ISO 27001:2013 aplicado de la Norma ISO 27001:2013**
AM10	**A.11.2.2 Servicios de suministro**
AM20	**A.8.1.2 Propiedad de los activos**
	A.8.3.2 Disposición de los medios
	A.8.3.3 Transferencia de los medios físicos
	A.9.2.6 Retiro o ajuste de los derechos de acceso
AM32	**A.8.1.1 Inventario de Activos**
	A.8.1.2 Propiedad de los activos
	A.11.2.8 Equipos de usuarios desatendido
AM37	**A.9.1.1 Política de control del acceso**
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM38	**A.12.1.1 Procedimientos de operación documentados**
	A.12.1.2 Gestión de cambios
AM51	**A.8.1.1 Inventario de Activos**
	A.8.1.2 Propiedad de los activos

Fuente: Autores.

Cuadro 49. Activo 2 vs controles ISO 27001:2013

A2 - Licencias de sistemas operativos windows	
Amenazas	**Descripción del control aplicado de la Norma ISO 27001:2013**
AM21	A.12.5.1 Instalación de software en sistemas operativos
AM27	A.12.4.2 Protección de la información del registro
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación
AM39	A.12.2.1 Controles contra códigos maliciosos
AM41	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM42	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM45	A.13.1.2 Seguridad de los servicios de red
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM46	A.12.2.1 Controles contra códigos maliciosos
	A.12.4.1 Registro de eventos
AM47	A.12.3.1 Respaldo de la información
AM48	A.12.5.1 Instalación de software en sistemas operativos
	A.12.6.2 Restricciones sobre la instalación de software

Fuente: Autores.

Cuadro 50. Activo 3 vs controles ISO 27001:2013

A3 - Licencias para servidores oracle	
Amenazas	**Descripción del control aplicado de la Norma ISO 27001:2013**
AM21	A.12.5.1 Instalación de software en sistemas operativos
AM27	A.12.4.2 Protección de la información del registro
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación
AM39	A.12.2.1 Controles contra códigos maliciosos
AM41	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM42	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM45	A.13.1.2 Seguridad de los servicios de red
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM46	A.12.2.1 Controles contra códigos maliciosos
	A.12.3.1 Respaldo de la información
AM47	A.12.3.1 Respaldo de la información
AM48	A.12.5.1 Instalación de software en sistemas operativos
	A.12.6.2 Restricciones sobre la instalación de software

Fuente: Autores.

Cuadro 51. Activo 4 vs controles ISO 27001:2013

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM9	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información
	A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas
	A.14.1.3 Protección de transacciones de los Servicios de las aplicaciones
AM17	A.12.4.3 Registros de administrador y de operador
	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información
	A.14.2.2 Procedimiento de control de cambios en sistemas
	A.12.4.3 Registros de administrador y de operador
	A.14.2.7 Desarrollo contratado externamente
	A.15.1.1 Política de seguridad de la información para las relaciones con los proveedore
	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
	A.16.1.3 Reporte de debilidades de seguridad de la información
	A.17.1.1 Planificación de la continuidad de las seguridad de la información
	A.17.1.2 Implementación de la continuidad de la seguridad de la información
	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
	A.18.1.3 Protección de registros
	A.18.1.4 Privacidad y protección de información de datos personales

Fuente: Autores.

Cuadro 51. Activo 4 vs controles ISO 27001:2013 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM21	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
	A.9.2.4 Gestión de información de autenticación secreta de usuarios
	A.9.2.5 Revisión de los derechos de acceso de usuarios
	A.9.3.1 Uso de información de autenticación secreta
	A.9.4.1 Restricción de acceso a la información
	A.12.2.1 Controles contra códigos maliciosos
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.3 Registros de administrador y de operador
	A.12.4.4 Sincronización de relojes
	A.16.1.1 Responsabilidades y procedimientos
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM22	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A.12.4.4 Sincronización de relojes
	A.13.1.1 Controles de las redes
AM23	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A.12.4.4 Sincronización de relojes
	A.13.1.1 Controles de las redes

Fuente: Autores.

Cuadro 51. Activo 4 vs controles ISO 27001:2013 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM26	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.3 Registros de administrador y de operador
	A.12.4.4 Sincronización de relojes
AM36	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
AM40	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
AM41	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.3 Registros de administrador y de operador
	A.12.4.4 Sincronización de relojes

Fuente: Autores.

Cuadro 51. Activo 4 vs controles ISO 27001:2013 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM42	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ell
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM45	A.13.1.2 Seguridad de los servicios de red
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ell
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM46	A.12.2.1 Controles contra códigos maliciosos
	A.12.5.1 Instalación de software en sistemas operativos

Fuente: Autores.

Cuadro 52. Activo 7 vs controles ISO 27001:2013

A7 - Routers y switch	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM12	A.11.2.4 Mantenimiento de equipos
AM25	A.12.4.2 Protección de la información del registro
AM27	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
AM37	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM38	A.12.1.3 Gestión de capacidad
AM43	A.8.3.3 Transferencia de los medios físicos
	A.13.2.1 Política y procedimientos de transferencia de información
	A.13.2.2 Acuerdos sobre transferencia de información
	A.13.2.3 Mensajería electrónica
AM45	A.13.1.2 Seguridad de los servicios de red
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ell
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM47	A.13.2.1 Política y procedimientos de transferencia de información

Fuente: Autores.

Cuadro 53. Activo 8 vs controles ISO 27001:2013

A8 - Modem	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM23	A.9.1.2 Acceso a redes y a servicios en red
AM31	A.11.2.4 Mantenimiento de equipos
	A.11.2.7 Disposición segura o reutilización de equipos
AM41	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM47	A.13.2.1 Política y procedimientos de transferencia de información

Fuente: Autores.

Cuadro 54. Activo 9 vs controles ISO 27001:2013

A9 - Cableado UTP	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM12	**A.11.2.3 Seguridad del cableado**
AM27	**A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones**
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
AM42	**A.15.1.1 Política de seguridad de la información para las relaciones con los proveedores**
	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
AM47	**A.13.2.1 Política y procedimientos de transferencia de información**

Fuente: Autores.

Cuadro 55. Activo 10 vs controles ISO 27001:2013

A10 - Servidor base de datos ARCA	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM11	A.12.3.1 Respaldo de la información
AM31	A.11.2.4 Mantenimiento de equipos
	A.11.2.7 Disposición segura o reutilización de equipos
AM37	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM42	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM52	A.6.1.3 Contacto con las autoridades
	A.6.1.4 Contacto con grupos de interés especial
	A.9.1.1 Política de control del acceso
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
	A.9.4.3 Sistema de gestión de contraseñas
	A.10.1.2 Gestión de llaves
	A.12.1.2 Gestión de cambios

Fuente: Autores.

Cuadro 56. Activo 11 vs controles ISO 27001:2013

A11 - Servidor de la aplicación web	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM11	A.12.3.1 Respaldo de la información
AM31	A.11.2.4 Mantenimiento de equipos
	A.11.2.7 Disposición segura o reutilización de equipos
AM37	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM42	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM52	A.6.1.3 Contacto con las autoridades
	A.6.1.4 Contacto con grupos de interés especial
	A.9.1.1 Política de control del acceso
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
	A.9.4.3 Sistema de gestión de contraseñas
	A.10.1.2 Gestión de llaves
	A.12.1.2 Gestión de cambios

Fuente: Autores.

Cuadro 57. Activo 12 vs controles ISO 27001:2013

A12 - Servidor de back-up	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM17	A.11.2.1 Ubicación y protección de los equipos
	A.12.4.4 Sincronización de relojes
AM32	A.8.1.1 Inventario de Activos
	A.8.1.2 Propiedad de los activos
	A.11.2.4 Mantenimiento de equipos
AM37	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM42	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM52	A.6.1.3 Contacto con las autoridades
	A.6.1.4 Contacto con grupos de interés especial
	A.9.1.1 Política de control del acceso
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
	A.9.4.3 Sistema de gestión de contraseñas
	A.10.1.2 Gestión de llaves
	A.12.1.2 Gestión de cambios

Fuente: Autores.

Cuadro 58. Activo 13 vs controles ISO 27001:2013

A13 - Firewall	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM9	A.11.2.1 Ubicación y protección de los equipos
AM21	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
	A.9.2.4 Gestión de información de autenticación secreta de usuarios
	A.9.2.5 Revisión de los derechos de acceso de usuarios
	A.9.3.1 Uso de información de autenticación secreta
	A.9.4.1 Restricción de acceso a la información
	A.12.2.1 Controles contra códigos maliciosos
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.3 Registros de administrador y de operador
	A.12.4.4 Sincronización de relojes
	A.12.5.1 Instalación de software en sistemas operativos
	A.13.1.1 Controles de las redes
	A.13.1.2 Seguridad de los servicios de red
	A.13.1.3 Separación en las redes
	A.16.1.1 Responsabilidades y procedimientos
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia

Fuente: Autores.

Cuadro 58. Activo 13 vs controles ISO 27001:2013 (Continuación)

A13 - Firewall	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM22	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A.12.4.4 Sincronización de relojes
	A.13.1.1 Controles de las redes
AM23	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A.12.4.4 Sincronización de relojes
	A.13.1.1 Controles de las redes
AM25	A.13.2.1 Política y procedimientos de transferencia de información
AM26	A.12.4.2 Protección de la información del registro
	A.12.4.3 Registros de administrador y de operador
	A.12.4.4 Sincronización de relojes
	A.12.4.1 Registro de eventos
AM27	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
AM28	A.12.6.1 Control de las vulnerabilidades técnicas
AM36	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
AM37	A.9.1.1 Política de control del acceso
	A.9.1.2 Acceso a redes y a servicios en red
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado
AM38	A.12.1.1 Procedimientos de operación documentados
	A.12.1.2 Gestión de cambios
	A.12.1.3 Gestión de capacidad

Fuente: Autores.

Cuadro 58. Activo 13 vs controles ISO 27001:2013 (Continuación)

A13 - Firewall	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM39	A.12.2.1 Controles contra códigos maliciosos
AM40	A.12.2.1 Controles contra códigos maliciosos
	A.12.1.2 Gestión de cambios
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
AM41	A.12.1.1 Procedimientos de operación documentados
AM42	A.12.1.2 Gestión de cambios
AM45	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM46	A.12.2.1 Controles contra códigos maliciosos
	A.12.5.1 Instalación de software en sistemas operativos
AM47	A.13.2.1 Política y procedimientos de transferencia de información
AM48	A.12.6.2 Restricciones sobre la instalación de software

Fuente: Autores.

Cuadro 59. Activo 14 vs controles ISO 27001:2013

A14 - Rack de datos	
Amenazas	**Descripción del control aplicado de la Norma ISO 27001:2013**
AM1	A.11.2.1 Ubicación y protección de los equipos
AM2	A.11.2.1 Ubicación y protección de los equipos
AM3	A.11.1.4 Protección contra amenazas externas y ambientales
	A.11.2.1 Ubicación y protección de los equipos
AM4	A.11.2.1 Ubicación y protección de los equipos
AM5	A.11.2.1 Ubicación y protección de los equipos
	A.11.2.5 Retiro de activos
	A.11.2.8 Equipos de usuarios desatendido
AM6	A.11.2.1 Ubicación y protección de los equipos
AM9	A.11.2.4 Mantenimiento de equipos
AM10	A.11.2.2 Servicios de suministro
AM11	A.11.2.1 Ubicación y protección de los equipos
	A.11.2.4 Mantenimiento de equipos
AM20	A.8.3.2 Disposición de los medios
	A.8.3.3 Transferencia de los medios físicos
	A.9.1.1 Política de control del acceso
	A.9.2.6 Retiro o ajuste de los derechos de acceso

Fuente: Autores.

Cuadro 59. Activo 14 vs controles ISO 27001:2013 (Continuación)

A14 - Rack de datos	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM32	A.8.1.2 Propiedad de los activos
	A.11.2.8 Equipos de usuarios desatendido
AM42	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM52	A.6.1.3 Contacto con las autoridades
	A.6.1.4 Contacto con grupos de interés especial
	A.8.1.1 Inventario de Activos
	A.8.1.2 Propiedad de los activos
	A.9.1.1 Política de control del acceso
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.3 Gestión de derechos de acceso privilegiado

Fuente: Autores.

Cuadro 60. Activo 17 vs controles ISO 27001:2013

A17 - Administrador del sistema	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM27	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	A.7.2.3 Proceso disciplinario
AM33	A.7.1.1 Selección
AM54	A.7.1.1 Selección
	A.8.2.3 Manejo de activos
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Fuente: Autores.

Cuadro 61. Activo 18 vs controles ISO 27001:2013

A18 - Administrador de la base de datos	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM27	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	A.7.2.3 Proceso disciplinario
AM33	A.7.1.1 Selección
AM54	A.7.1.1 Selección
	A.8.2.3 Manejo de activos
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Fuente: Autores.

Cuadro 62. Activo 19 vs controles ISO 27001:2013

A19 - Selección y contratación (docentes, administrativos)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM20	A.7.1.1 Selección
	A.7.1.2 Términos y condiciones de empleo
	A.7.2.1 Responsabilidades de la dirección
	A.7.2.3 Proceso disciplinario
	A.7.3.1 Terminación o cambio de responsabilidades de empleo
	A.9.1.1 Política de control del acceso
	A.9.2.1 Registro de usuarios y cancelación del registro de usuarios
	A.9.2.2 Suministro de acceso de usuarios
	A.9.2.5 Revisión de los derechos de acceso de usuarios
	A.9.2.6 Retiro o ajuste de los derechos de acceso
AM27	A.7.1.1 Selección
	A.7.2.1 Responsabilidades de la dirección
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Fuente: Autores.

Cuadro 63. Activo 20, 21 y 22 vs controles ISO 27001:2013

A20 - Persona que actua e interactua dentro del sistema y la organización (docente)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM54	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	A.7.2.3 Proceso disciplinario
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

A21 - Persona que actua e interactua dentro del sistemay la organización (estudiante)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM54	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	A.7.2.3 Proceso disciplinario
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

A22 - Persona que actua e interactua dentro del sistema y la organización (Registro acad)	
Amenazas	**Descripción del control aplicado de la norma ISO 27001:2013**
AM54	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	A.7.2.3 Proceso disciplinario
AM55	A.7.1.2 Términos y condiciones de empleo
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Fuente: Autores.

- **La explicación de los controles a implementar en el módulo Gradebook del sistema de información académico[50] para cada activo, se presentan desde el cuadro 64 al 76:**

Cuadro 64. Control explicado para el activo 1

A1 - Equipos de computo docentes, administrativos y estudiantes		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C1	A.8.1.1	Se deben identificar los activos de la universidad relacionados con el modulo Gradebook que están asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos.
C2	A.8.1.2	Todos los Activos mantenidos en el inventario deben tener un propietario.
C3	A.8.3.2	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
C4	A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
C5	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C6	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C7	A.9.2.1	Se debe implementar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C8	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C9	A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo o se deben ajustar cuando se realicen cambios.
C10	A.11.2.2	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros), ej.: Pararrayos.
C11	A.11.2.8	Los usuarios deben asegurarse de que a los equipos desatendidos se les de protección apropiada.
C12	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C13	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.

Fuente: Autores.

[50] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Anexo A. Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2013, 13-24 p. (NTC-ISO/IEC 27001).

Cuadro 65. Control explicado para el activo 2 – 3

A2 - Licencias de sistemas operativos windows / A3 - Licencias para servidores oracle		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C14	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C15	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C16	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos malicioso (ej.: Gusanos, troyanos, ransomware).
C17	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).
C18	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe estable una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C19	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C20	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. (Ej.: Sincronizar con reloj mundial).
C21	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos (generar alertas en caso de activación de proceso de instalación).
C22	A.12.6.2	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. (Generar Política de Instalación de Software en los equipos de la Universidad).
C23	A.13.1.2	Se deben identificar los mecanismo de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraen externamente.

Fuente: Autores.

Cuadro 65. Control explicado para el activo 2 – 3 (Continuación)

A2 - Licencias de sistemas operativos windows / A3 - Licencias para servidores oracle		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C24	A.15.1.3	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologia de información y comunicación. (Politica Protección de datos
C25	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C26	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
C27	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimeintos documentados (Apobados por Calidad).
C28	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Autores.

Cuadro 66. Control explicado para el activo 4

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C29	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C30	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C31	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej.: Implementar en el Paz y Salvo la firma de Informática para cerrar cuenta email, usuarios Sistema de Información académico, contable y mesa de ayuda).
C32	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C33	A.9.2.4	La asignación de la información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. (Ej:envio de Email con archivo cifrado)
C34	A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
C35	A.9.3.1	Se deben exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
C36	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
C37	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C38	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C39	A.12.1.4	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe estable una clausula en el contrato donde se le informe al usuario
C40	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos malicioso (ej.: Gusanos, troyanos, ransomware).
C41	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).

Fuente: Autores.

Cuadro 66. Control explicado para el activo 4 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C29	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C30	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C31	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej.: Implementar en el Paz y Salvo la firma de Informática para cerrar cuenta email, usuarios Sistema de Información académico, contable y mesa de ayuda).
C32	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C33	A.9.2.4	La asignación de la información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. (Ej:envio de Email con archivo cifrado)
C34	A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
C35	A.9.3.1	Se deben exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
C36	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
C37	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C38	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C39	A.12.1.4	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe estable una clausula en el contrato donde se le informe al usuario
C40	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos malicioso (ej.: Gusanos, troyanos, ransomware).

Fuente: Autores.

Cuadro 66. Control explicado para el activo 4 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C41	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).
C42	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe estable una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C43	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C44	A.12.4.3	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
C45	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. (Ej.: Sincronizar con reloj mundial).
C46	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos (generar alertas en caso de activación de proceso de instalación).
C47	A.13.1.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
C48	A.13.1.2	Se deben identificar los mecanismo de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraen externamente.
C49	A.14.1.1	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
C50	A.14.1.2	La información involucrada en los servicios de las aplicaciones que pasan sobre redes publicas se deben proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizada.

Fuente: Autores.

Cuadro 66. Control explicado para el activo 4 (Continuación)

A4 - Sistema de Información PeopleSoft - ARCA (GradeBook)		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C51	A.14.1.3	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no
C52	A.14.2.2	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante uso de procedimientos formales de control de cambios (establecer procedimientos de cambios controlados)
C53	A.14.2.7	La organización debe supervisar y hacer seguimeinto de la actividad de desarrollo de sistemas contratados externamente. (Generar Reunión de seguimiento donde se realice levantamiento de acta identificando cada seguimiento y avance del proyecto)
C54	A.15.1.1	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
C55	A.15.1.2	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. (Ej: Establecer
C56	A.16.1.1	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficazy ordenada a los incidentes de seguridad de la Información.
C57	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C58	A.16.1.3	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la Universidad, que observen o reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistema o servicios (trafico de notas entre
C59	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.

Fuente: Autores.

Cuadro 66. Control explicado para el activo 4 (Continuación)

A4 - Sistema de información PeopleSoft - ARCA (GradeBook)		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C60	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimientos documentados (Aprobados por Calidad).
C61	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
C62	A.17.1.1	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
C63	A.17.1.2	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
C64	A.18.1.1	Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la universidad. (ejemplo Reglamento Estudiantil, PEI y derechos pecuniarios)
C65	A.18.1.3	Los registros se deben proteger contra pérdida, destrucción, falsificación, accesos liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
C66	A.18.1.4	Se debe asegurar la privacidad y la protección de la información de datos personales como se exige en la legislación y la reglamentación pertinente, cuando sea aplicable, esto se puede aplicar a través de la Ley (1581, protección de datos)

Fuente: Autores.

Cuadro 67. Control explicado para el activo 7

A7 - Routers y switch		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C67	A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el tranporte.
C68	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en gradebook).
C69	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales hansido autorizados. (Basados en el rol para el cual fue contratada a persona).
C70	A.9.2.1	Se debe implmentar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C71	A.9.2.3	Se debe restringir y controlar la asignacion y uso de derechos de acceso privilegiado (ej: Coordinador, Secretaria Gral, Decanos).
C72	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C73	A.11.2.6	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
C74	A.12.1.3	Se debe hacer seguimiento al uso de recursos, hacer ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
C75	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe establer una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C76	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C77	A.13.1.2	Se deben identificar los mecanismo de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraen externamente.

Fuente: Autores.

Cuadro 67. Control explicado para el activo 7 (Continuación)

A7 - Routers y switch		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C78	A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
C79	A.13.2.2	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
C80	A.13.2.3	Se debe proteger adecuadamente la información incluida en la mensjaería electrónica.
C81	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C82	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
C83	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimeintos documentados (Apobados por Calidad).
C84	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información

Fuente: Autores.

Cuadro 68. Control explicado para el activo 8

A8 - Modem		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C85	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales hansido autorizados. (Basados en el rol para el cual fue contratada a persona).
C86	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C87	A.11.2.7	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.
C88	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C89	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesmiento de información (ARCA) que afectan la seguridad de la información.
C90	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una politica de copias de respaldo acordadas (Ej: Cronograma de Ejecución de copias y verificación de las mismas).
C91	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe establer una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C92	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C93	A.12.4.4	Los relojes de todos los sistemas de prosamiento de información pertinentes dentro de una organizacióno ámbito de seguridad se deben sincronizar con una unica fuente de referencia de tiempo. (Ej: Sincronizar con reloj mundial).
C94	A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

Fuente: Autores.

Cuadro 69. Control explicado para el activo 9

A9 - Cableado UTP		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C95	A.11.2.3	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se deben proteger contra interceptación, interferencia o daño.
C96	A.11.2.6	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
C97	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe establecer una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C98	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C99	A.13.2.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
C100	A.15.1.1	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
C101	A.15.1.2	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. (Ej.: Establecer requisitos de conexión a proveedor desarrollador que este realizando mejoras al sistema).

Fuente: Autores.

Cuadro 70. Control explicado para el activo 10 – 11

A10 - Servidor base de datos ARCA / A11 - Servidor de la aplicación web		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C102	A.6.1.3	Se deben mantener contactos apropiados con las autoridades pertinentes
C103	A.6.1.4	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
C104	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C105	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C106	A.9.2.1	Se debe implementar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C107	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej.: Implementar en el Paz y Salvo la firma de Informática para cerrar cuenta email, usuarios Sistema de Información académico, contable y mesa de ayuda).
C108	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C109	A.9.4.3	Los sistemas de gestión de contraseña deben ser interactivos y deben asegurar la calidad de las contraseñas.
C110	A.10.1.2	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
C111	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C112	A.11.2.7	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.
C113	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C114	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).

Fuente: Autores.

Cuadro 70. Control explicado para el activo 10 – 11 (Continuación)

A10 - Servidor base de datos ARCA / A11 - Servidor de la aplicación web		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C111	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C112	A.11.2.7	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.
C113	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C114	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).
C115	A.15.1.2	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la
C116	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C117	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
C118	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimientos documentados (Aprobados por Calidad).
C119	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Autores.

Cuadro 71. Control explicado para el activo 12

A12 - Servidor de backups		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C120	A.6.1.3	Se deben mantener contactos apropiados con las autoridades pertinentes
C121	A.6.1.4	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
C122	A.8.1.1	Se deben identificar los activos de la universidad relacionados con el modulo Gradebook que están asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos.
C123	A.8.1.2	Todos los Activos mantenidos en el inventario deben tener un propietario.
C124	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C125	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C126	A.9.2.1	Se debe implementar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C127	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej.: Implementar en el Paz y Salvo la firma de Informática para cerrar
C128	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C129	A.9.4.3	Los sistemas de gestión de contraseña deben ser interactivos y deben asegurar la calidad de las contraseñas.
C130	A.10.1.2	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
C131	A.11.2.1	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
C132	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C133	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.
C134	A.12.4.4	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).

Fuente: Autores.

Cuadro 71. Control explicado para el activo 12 (Continuación)

A12 - Servidor de backups		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C135	A.15.1.2	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener
C136	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C137	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
C138	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimientos documentados (Aprobados por Calidad).
C139	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Autores.

Cuadro 72. Control explicado para el activo 13

A13 - Firewall		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C140	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en Gradebook).
C141	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales han sido autorizados. (Basados en el rol para el cual fue contratada a persona).
C142	A.9.2.1	Se debe implementar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C143	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej.: Implementar en el Paz y Salvo la firma de Informática para cerrar
C144	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado (ej.: Coordinador, Secretaria Gral., Decanos).
C145	A.9.2.4	La asignación de la información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. (Ej:envio de Email con archivo cifrado)
C146	A.9.2.5	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
C147	A.9.3.1	Se deben exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
C148	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
C149	A.11.2.1	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
C150	A.11.2.6	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
C151	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C152	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej.: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesamiento de información (ARCA) que afectan la seguridad de la información.

Fuente: Autores.

Cuadro 72. Control explicado para el activo 13 (Continuación)

A13 - Firewall		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C153	A.12.1.3	Se debe hacer seguimiento al uso de recursos, hacer ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
C154	A.12.1.4	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe establecer una clausula en el contrato donde se le informe al usuario q
C155	A.12.2.1	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos malicios (ej.: Gusanos, troyanos, ransomware).
C156	A.12.3.1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas (Ej.: Cronograma de Ejecución de copias y verificación de las mismas).
C157	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la Información. (Previo a esto se debe establer una clausula en el contrato donde se le informe al usuario que todas sus actividades relacionadas con los activos de información vana ser registradas para realizar seguimientos).
C158	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteraciones y accesos no autorizados. (Solicitando claves de acceso al iniciar sesión, huellas dactilar al ingresar a las instalaciones).
C159	A.12.4.3	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
C160	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organizacióno ámbito de seguridad se deben sincronizar con una unica fuente de referencia de tiempo. (Ej: Sincronizar con reloj mundial).
C161	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos (generar alertas en caso de activación de proceso de instalación).

Fuente: Autores.

Cuadro 72. Control explicado para el activo 13 (Continuación)

A13 - Firewall		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C162	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organziación a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
C163	A.12.6.2	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. (Generar Politica de Instalación de Software en los equipos de la Universidad).
C164	A.13.1.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
C165	A.13.1.2	Se deben identificar los mecanismo de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraen externamente.
C166	A.13.1.3	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
C167	A.13.2.1	mediante el uso de todo tipo de instalaciones de comunicaciones. (Establecer alertas en caso de instalación de cualquier software en los equipos de la Universidad)
C168	A.16.1.1	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficazy ordenada a los incidentes de seguridad de la Información.
C169	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C170	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimeintos documentados (Apobados por Calidad).
C171	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Autores.

Cuadro 73.Control explicado para el activo 14

A14 - Rack de datos		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C172	A.6.1.3	Se deben mantener contactos apropiados con las autoridades pertienentes
C173	A.6.1.4	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
C174	A.8.1.1	Se deben identificar los activos de la universidad relacionados con el modulo Gradebook que estan asociados con información e instlaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos.
C175	A.8.1.2	Todos los Activos mantenidos en el inventario deben tener un propietario.
C176	A.8.3.2	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
C177	A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
C178	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en gradebook).
C179	A.9.2.1	Se debe implmentar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C180	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas o servicios. (Ej: Implementar en el Paz y Salvo la firma de Informática para cerrar cuenta email, usuarios Sistema de Información académico, contable y mesa de ayuda).
C181	A.9.2.3	Se debe restringir y controlar la asignacion y uso de derechos de acceso privilegiado (ej: Coordinador, Secretaria Gral, Decanos).
C182	A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo o se deben ajustar cuando se realicen cambios.
C183	A.11.1.4	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentales.
C184	A.11.2.1	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
C185	A.11.2.2	Los equipos se deben proteger contra fallas de energía y otras interrupciones casusadas por fallas en los servicios de suministros),
C186	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Fuente: Autores.

Cuadro 73. Control explicado para el activo 14 (Continuación)

A14 - Rack de datos		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C186	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
C187	A.11.2.5	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
C188	A.11.2.8	Los usuarios deben asegurarse de que a los equipos desatendidos se les de protección apropiada.
C189	A.15.1.2	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. (Ej: Establecer requisitos de conexión a proveedor desarrollador que este realizando mejoras al sistema).
C190	A.16.1.2	Los eventos seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
C191	A.16.1.4	Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
C192	A.16.1.5	Se debe dar respuesta a los incidentes de seguridad de la Información de acuerdo con procedimeintos documentados (Apobados por Calidad).
C193	A.16.1.7	La universidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Fuente: Autores.

Cuadro 74. Control explicado para el activo 17 – 18

A17 - Administrador del Sistema / A18 - Administrador de la Base de Datos		
Nº Control	**# ISO 27001:2013**	**Descripción del control a aplicar**
C194	A.7.1.1	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes,
C195	A.7.1.2	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
C196	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre políticas y procedimeintos de la universidad pertinentes para el cargo.

Fuente: Autores.

Cuadro 75. Control explicado para el activo 19

A19 - Selección y contratación (Docentes, administrativos)		
Nº Control	# ISO 27001:2013	Descripción del control a aplicar
C199	A.7.1.1	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
C200	A.7.1.2	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
C201	A.7.2.1	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la informaciónde acuerdo con las politicas y procedimientos establecidos por la universidad.
C202	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre políticas y procedimeintos de la universidad pertinentes para el cargo.
C203	A.7.2.3	Se debe contar con un proceso formal; el cual debe ser comunicado, para empreder acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Fuente: Autores.

Cuadro 76. Control explicado para el activo 20 – 21 – 22

A20 - Persona que actua e interactua dentro del sistema y la organización (docente) / A21 (estudiante) / A22 (registro y control)		
Nº Control	# ISO 27001:2013	Descripción del control a aplicar
C210	A.7.1.2	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
C211	A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre políticas y procedimeintos de la universidad pertinentes para el cargo.
C212	A.7.2.3	Se debe contar con un proceso formal; el cual debe ser comunicado, para empreder acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Fuente: Autores.

7. POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LOS ACTIVOS MÁS SIGNIFICATIVOS DEL MÓDULO GRADEBOOK EN EL SISTEMA ACADÉMICO

Las políticas de Seguridad de la Información, serán las directrices que deben cumplir los usuarios, administradores y terceros que hacen uso del módulo Gradebook del sistema ARCA y demás custodios de los activos asociados, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad de la información generada.

Están orientadas a proteger los activos de información en todos los ambientes, internos y externos, en los cuales se almacenan, procesan, transmiten, operan o usan y procuran mantener los controles correspondientes para su adecuada protección; de la misma forma contribuyen a minimizar los riesgos de una eventual pérdida de los activos de información especialmente los más sensitivos del módulo Gradebook.

Por lo anterior, se proponen las siguientes Políticas Generales en Seguridad de la Información, basados en la norma ISO 27001:2013, las cuales ayudarán a ofrecer la información del sistema de notas de manera segura y confiable.

Estas políticas deben ser informadas, socializadas y promovidas como de estricto cumplimiento para los actores asociados a los activos definidos en la fase inicial de éste proyecto.

7.1 POLÍTICAS GENERALES

Objetivo de control A.5. Políticas de Seguridad de la Información

7.1.1 POLGRAL001. Los directivos del departamento TIC evaluarán las situaciones que hayan dado lugar a un incumplimiento a las Políticas de Seguridad de la Información, recomendará las acciones a seguir, para mantener el modelo de Seguridad de la Información propuesto para el módulo Gradebook. En el mismo sentido será el encargado de aprobar modificaciones o nuevas políticas de seguridad de la información.

7.1.2 POLGRAL002. El área informática deberá presentar estrategias técnica y económicamente viables que faciliten el cumplimiento de las políticas de seguridad de la información planteadas en el presente documento.

7.1.3 POLGRAL003. Todos los usuarios y administradores que tengan acceso a la plataforma tecnológica del módulo Gradebook del sistema ARCA, deberán conocer y cumplir las políticas de seguridad de la información y éstas deberán ser informadas de manera escrita por medio de mensaje de datos. Los usuarios y administradores deben entregar soporte de haberlas recibido, entendido antes de recibir su usuario y contraseña.

7.1.4 POLGRAL004. Todos los usuarios y en especial los administradores que identifiquen cualquier anomalía en la plataforma Gradebook o en alguno de los activos identificados deberán reportarla al departamento TIC por escrito, para garantizar una constante retroalimentación y un proceso de mejora continua

7.1.5 POLGRAL005. El área de informática podrá utilizar herramientas para identificar problemas y mejorar el uso adecuado de las tecnologías de información y comunicaciones del módulo Gradebook del sistema ARCA.

7.1.6 POLGRAL006. El departamento TIC nombrará a un coordinador de seguridad informática con las capacidades técnicas y cualidades en la facilidad de transferencia de información verbal y escrita cuyas funciones específicas están descritas en la POLRES02 del presente documento, este a su vez debe contar con el reconocimiento y apoyo del personal que asigne el departamento TIC para ejecutar sus funciones.

7.2 POLÍTICAS DE ASIGNACIÓN DE RESPONSABILIDADES

Objetivo de control A.6. Organización de la Seguridad de la Información

Las siguientes políticas describen los roles y responsabilidades de los usuarios del módulo Gradebook, los cuales se enumerarán con la sigla POLRES:

7.2.1 POLRES01. Consejo superior es el responsable que los usuarios a su cargo, conozcan y apliquen las políticas de seguridad de la información. En ese sentido deben exigir que todo administrador, usuario o terceras partes que tengan acceso a los activos de información del módulo Gradebook, cumplan las políticas y los procedimientos de seguridad de la información establecidos por el módulo Gradebook del sistema ARCA.

7.2.2 POLRES02. Coordinador de Seguridad Informática: El rol del coordinador de Seguridad Informática es la figura que organiza, planea y promueve las actividades que tengan que ver con la Seguridad Informática.

7.2.3 POLRES03. Responsable de la Información: Las dependencias asociadas a cada uno de los procesos trasversales del módulo Gradebook del sistema ARCA son las responsables de la información necesaria, para el cumplimiento de las funciones emanadas en el reglamento interno de la UECCI.

7.2.4 POLRES04. Perfil Administrador: Los administradores tienen la responsabilidad de hacer el uso correcto de sus privilegios, de acuerdo a las políticas de los activos de información y de los servicios que estén a su cargo.

7.2.5 POLRES05. Perfil Usuarios: Los usuarios del sistema ARCA, que hacen uso de los servicios o aplicativos informáticos del módulo Gradebook son responsables de dar un uso apropiado a los activos conforme a lo establecido en el reglamento interno de la UECCI. Todo usuario del módulo Gradebook del sistema ARCA es responsable por el cumplimiento de las políticas de seguridad de la información. Adicionalmente está comprometido a reportar al personal de TIC de la Universidad cualquier incidente de seguridad del que tenga conocimiento, por los medios y formas establecidos para ello.

7.2.6 POLRES06. Los terceros que tengan acceso a los activos de información tecnológicos, están obligados a cumplir las políticas de Seguridad de la Información del módulo Gradebook del sistema ARCA, y tienen las mismas responsabilidades que los usuarios internos de los aplicativos y servicios informáticos. Se debe asegurar que dentro de los contratos de servicios se incluya una cláusula de confidencialidad y cumplimiento de políticas de seguridad debidamente abalada por el departamento jurídico de la UECCI.

7.3 POLITICAS RECURSOS HUMANOS

Objetivo de control A.7. Seguridad de los Recursos Humanos

Las siguientes políticas direccionan las condiciones de los recursos humanos que están implicados en el módulo Gradebook, durante su proceso de selección, ejecución del empleo y la terminación del respectivo contrato, las cuales se enumerarán con la sigla POLREHUM:

7.3.1 POLREHUM01. Todo el personal a contratar y que haga uso del módulo Gradebook en especial los proyectados para administradores deberá pasar por un proceso de selección riguroso que incluya revisión de antecedentes y confirmación de referencias de acuerdo a la ley vigente.

7.3.2 POLREHUM02. Los procesos disciplinarios y en especial los asociados a delitos informáticos deberán estar detallados en el contrato laboral de los empleados y serán socializados periódicamente por los medios que el consejo directivo determine.

7.3.3 POLREHUM03. Retiro de los derechos de acceso: cuando un usuario llámese estudiante, administrador o tercero termine su relación con la UECCI, se deben retirar las cuentas de acceso y éste deberá entregar los activos que pudieran ser asignados para el desempeño de su rol al área de la Universidad. Los accesos lógicos a los activos de información deben ser removidos por el administrador del sistema de forma inmediata y las cuentas de acceso deben colocarse en estado inactiva para los administradores por quince días (15) días, para los estudiantes por (10) días y para los terceros de manera inmediata.

7.4 POLÍTICAS DE GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Objetivo de control A.8. Gestión de Activos

Las siguientes políticas describen la responsabilidad por los activos, clasificación de información y manejo de medios asignados al módulo Gradebook del sistema ARCA los cuales se enumerarán con la sigla POLAI:

7.4.1 POLAI01. Inventario de activos de información: La UECCI mantendrá un inventario actualizado de los activos de información a través de la subdirección sdministrativa y el departamento de informática.

Entrega y reasignación de activos: El área TIC debe verificar la entrega de la información y su organización en los discos de red para garantizar su preservación y conservación en el momento de la salida o cambio de administrador. Antes de la asignación de un equipo que perteneció a un administrador retirado, se debe hacer limpieza de la información de manera segura.

7.4.2 POLAI02. Propietarios de los activos de información: La UECCI es propietaria de todos los activos de información tecnológicos, así como los datos creados, almacenados y recibidos en el módulo Gradebook. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la universidad, serán sancionadas de acuerdo con las normas legales vigentes. Los administradores de estos activos son responsables de salvaguardar la información producto de los procesos.

7.4.3 POLAI03. Uso aceptable de los activos: Los usuarios y administradores podrán utilizar únicamente en los equipos, los programas autorizados por la oficina de soporte informático de la UECCI.

Los recursos informáticos asignados al módulo Gradebook del sistema ARCA no podrán ser utilizados para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), material político, material religioso o cualquier otro uso que no esté autorizado.

El usuario, administradores o terceros que hagan uso del módulo Gradebook no deben realizar intencionalmente actos que impliquen un mal uso de los activos. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales.

Los administradores, usuarios o terceros no podrán efectuar cualquiera de las siguientes labores sin previa autorización del área de soporte informático de la Universidad:

a. Instalar software en cualquier equipo señalado como activo en el presente documento y en especial que sea parte del módulo Gradebook del sistema ARCA.

b. Bajar o descargar software de internet u otro servicio en línea en cualquier equipo señalado como activo en el presente documento y en especial que sea parte del módulo Gradebook del sistema ARCA.

c. Modificar, revisar, transformar o adaptar cualquier componente de software o equipo señalado como activo en el presente documento y en especial que sea parte del módulo Gradebook del sistema ARCA.

d. Descompilar o realizar ingeniería de reverso en cualquier software que sea parte del módulo Gradebook del sistema ARCA.

7.4.4 POLAI04. Responsabilidades sobre los activos: Ningún usuario, administrador o tercero podrá acceder al sistema de cómputo utilizando la cuenta y contraseña de otro usuario. El Usuario deberá informar a su jefe inmediato de cualquier conocimiento que tenga de alguna violación sobre el uso adecuado o legal del software o sobre los derechos respectivos de autor.

El Usuario es responsable de todas las transacciones o acciones efectuadas con su usuario. Cada usuario es responsable de asegurar que el uso de redes externas, tal como internet, no comprometa la seguridad de los recursos informáticos del módulo Gradebook del sistema ARCA. Esta responsabilidad incluye, pero no se limita a, prevenir que intrusos tengan acceso los recursos informáticos y de prevenir la introducción y propagación de virus.

Todo cambio a la infraestructura informática que incluya activos de información del módulo Gradebook deberá estar controlado y será realizado de acuerdo con los procedimientos definidos por el consejo superior, bajo los lineamientos de los administradores del módulo Gradebook del sistema ARCA antes de su ejecución.

La información del módulo Gradebook del sistema ARCA debe ser respaldada de forma frecuente (Diaria), dichos respaldos deben ser almacenados en lugares apropiados en los cuales la información esté segura y pueda ser recuperada en caso de un desastre natural, industrial o de incidentes con los equipos de procesamiento.

7.5 POLÍTICAS DE GESTIÓN DE ACCESO DE USUARIOS

Objetivo de control A.9. Control de Acceso

Las siguientes políticas describen los requisitos para el acceso a los activos asociados al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLACCE:

7.5.1 POLACCE01. El consejo superior debe establecer, documentar y revisar una política de control de accesos con base a las necesidades de seguridad de los activos asociados al módulo Gradebook.

7.5.2 POLACCE02. El área de datacenter debe proveer a los usuarios los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Se deben establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

7.5.3 POLACCE03. Los procedimientos a implementar para el acceso a los activos asociados al módulo Gradebook de ARCA deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso al módulo.

El área de informática debe prestar especial atención, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

7.5.4 POLACCE04. El área de informática debe procurar que los usuarios sean conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

7.5.5 POLACCE05. Las mesas de escritorio y monitores deben estar libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

7.5.6 POLACCE06. El área de informática de la UECCI debe implementar revisiones periódicas para incluir cualquier cambio que no estuviera documentado en los permisos de usuarios administradores o terceros que tienen acceso al módulo Gradebook.

7.5.7 POLACCE07. El área de gestión documental definirá la clasificación de la Información contenida en el modulo Gradebook y en busca de salvaguardar los niveles de confidencialidad el área de informática implementará los mecanismos necesarios para que dichos niveles no sean violados por usuarios no autorizados.

7.5.8 POLACCE08. Todas las contraseñas de cuentas que den acceso a recursos y servicios del módulo Gradebook deberán seguir las siguientes directrices generales:

a. Todas las contraseñas de sistema (root, administradores NT, cuentas de administración de aplicaciones, etc…) deben ser cambiados al menos una vez cada seis meses.

b. Todas las contraseñas de usuario deben ser cambiadas al menos una vez cada doce meses. Sin embargo, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.

c. La longitud de la contraseña no debe ser menor a 8 caracteres y debe incluir mínimo un número, una letra mayúscula, una letra minúscula y dos caracteres especiales.

d. Las cuentas de usuario que tengan privilegios del sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener contraseñas distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos.

e. Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas en conversaciones telefónicas.

f. En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les

comunicará a los usuarios su contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.

g. Las contraseñas por defecto asociadas al módulo Gradebook deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.

h. Todas las contraseñas de sistema, de usuario de recursos y servicios UPV deben respetar las recomendaciones descritas en la presente política. Algunos servicios en los que sea crítico el mantener la seguridad de la contraseña podrán determinar medidas adicionales de protección de la misma.

7.5.9 POLACCE09. Cualquier usuario o administrador que requiera acceso al código fuente de módulo Gradebook debe tener permiso por escrito del consejo superior en donde se indique la razón del acceso y los alcances máximos permitidos en dicho acceso.

7.6 POLÍTICAS SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Objetivo de control A.10. Criptografía

Las siguientes políticas describen los requisitos para el uso de controles criptográficos asociados al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLCRIP:

7.6.1 POLCRIP01. El área de dirección TIC definirá los mecanismos necesarios para proteger la confidencialidad, autenticidad o integridad de la información específicamente mediante la ayuda de técnicas criptográficas.

7.6.2 POLCRIP02. El área de informática evaluará e implementará los procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado cuando cumplan su ciclo de vida.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

7.7 POLÍTICAS SOBRE LA SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo de control A.11. Seguridad Física y del Entorno

Las siguientes políticas describen los requisitos para el uso de controles que soporte a la seguridad física y del entorno asociados a los activos al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLSEG:

7.7.1 POLSEG01. El área de datacenter debe evitar el acceso físico no autorizado, daño e interferencia con la información y los activos físicos asociados al módulo Gradebook de la organización. Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

7.7.2 POLSEG02. El área administrativa debe asegurar la retirada de todos los pases de empleado y de visita cuando se vayan e implementar los sistemas de acceso con tarjeta de esta forma rechacen y disparen una alarma ante intentos de acceso no autorizados.

7.7.3 POLSEG03. El área de seguridad debe implementar el uso de pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las 8 horas de haberse emitido. Las tarjetas de identificación deben mostrar colores para indicar las áreas accesibles por los visitantes (p. ej., azul para el primer piso, verde para el área administrativa, etc.;).

Cualquier miembro de la comunidad de la Universidad debe informar inmediatamente al área de seguridad en caso de ver algún visitante por fuera del área autorizada según el color de su pase de visita.

7.7.4 POLSEG04. El área de informática y de Datacenter deben evaluar, diseñar, e implementar controles para la protección física de los activos de información asociados al módulo Gradebook de ARCA.

7.7.5 POLSEG05. El área de datacenter y planta física debe garantizar el correcto suministro eléctrico a los activos de información y en los casos que sea necesario se debe contar con fuentes de energía redundantes online que permitan subsistir por lo menos 4 horas en caso de falla en el suministro principal de energía.

7.7.6 POLSEG06. El departamento de soporte informático debe diseñar e implementar formatos de retiro de activos y estos deben incluir espacios para firmas del administrador que autoriza el retiro de activos asociados al módulo Gradebook de su ubicación original.

7.7.7 POLSEG07. El área administrativa diseñará e implementará mantenimientos según las recomendaciones de los fabricantes de los activos de manera periódica. Para el diseño del plan, se debe contar con las recomendaciones del departamento de datacenter. Dichos mantenimientos deberán ser consultados e informados previamente a los administradores y ellos darán el aval para su ejecución en los tiempos y las condiciones que minimicen el tiempo sin servicio del módulo Gradebook.

7.8 POLÍTICAS SOBRE LA SEGURIDAD EN LAS OPERACIONES

Objetivo de control A.12. Seguridad de Operaciones

Las siguientes políticas proporcionan los lineamientos para la seguridad de las operaciones asociadas al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLOPE:

7.8.1 POLOPE01. Asignación de responsabilidades operativas: El área de Dirección TIC, será la encargada de la operación y administración de los activos tecnológicos que apoyan los procesos asociados al módulo Gradebook, en ese sentido asignará funciones específicas a los administradores, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los activos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre Gradebook, serán adecuadamente controlados y debidamente autorizados.

7.8.2 POLOPE02. El consejo superior de la UECCI debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

7.8.3 POLOPE03. El área de datacenter a través de los administradores, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (Capacity Planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica que soporta el módulo Gradebook. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

7.8.4 POLOPE04. El área de Dirección TIC propondrá al consejo superior de la UECCI los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente, ocasionados por el contagio de software malicioso específicamente sobre los activos asociados al Módulo Gradebook. Además, proporcionará los mecanismos para generar cultura de seguridad entre los usuarios, administradores y terceros.

7.8.5 POLOPE05. Política de copias de respaldo de la información. El área de Datacenter certificará la generación de copias de respaldo y almacenamiento de la información crítica contenida en el módulo Gradebook, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de procesos asociados con Gradebook, con el apoyo del área de Datacenter, serán los encargados de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, el área de Datacenter velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

7.8.6 POLOPE06. El área de informática, en conjunto con el consejo superior, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos asociados al módulo Gradebook.

Los administradores, deben habilitar los registros de auditoría y sistemas de monitoreo de la plataforma que sustenta Gradebook, acorde con los eventos a auditar preestablecidos por el área de informática.

7.9 POLÍTICAS SOBRE LA SEGURIDAD EN LAS COMUNICACIONES

Objetivo de control A.13. Seguridad de Operaciones

Las siguientes políticas proporcionan los lineamientos para la seguridad en las comunicaciones asociadas al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLCOM:

7.9.1 POLCOM01. EL consejo superior establecerá, a través de área redes, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios asociados al módulo Gradebook; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

7.9.2 POLCOM02. El área de redes debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red base para Gradebook. Así mismo debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos asociadas a la aplicación en estudio.

7.9.3 POLCOM03. El administrador de infraestructura debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el módulo Gradebook del sistema ARCA.

7.10 POLÍTICAS SOBRE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo de control A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas

Las siguientes políticas proporcionan los lineamientos para adquisición, desarrollo y mantenimiento de sistemas asociados al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLAD:

7.10.1 POLAD01. La UECCI asegurará que el software adquirido y desarrollado tanto al interior de la Universidad, como por terceras partes, para apoyar o complementar Gradebook, cumplirá con los requisitos de seguridad y calidad establecidos por él.

Las áreas propietarias de los procesos, en acompañamiento del área de informática deben establecer las especificaciones de adquisición o desarrollo de mejoras al módulo Gradebook, considerando requerimientos de seguridad de la información.

7.10.2 POLAD02. Las áreas propietarias de los procesos asociados a Gradebook deben definir qué información sensible puede ser eliminada del módulo y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

7.10.3 POLAD03. El área de informática debe liderar la definición de requerimientos de seguridad del módulo Gradebook, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

7.10.4 POLAD04. El desarrollador del módulo Gradebook deben certificar que el software entregado a la UECCI ha sido desarrollado utilizando herramientas licenciadas y reconocidas en el mercado.

7.10.5 POLAD05. Los propietarios de los procesos son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan el módulo Gradebook.

7.10.6 POLAD06. El área de datacenter debe asegurase que el software usado por el módulo Gradebook, cuente con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

Los controles y gestión de cambios en el módulo Gradebook y los activos asociados al mismo estarán a cargo del área de informática de la UECCI.

7.11 POLÍTICAS SOBRE LAS RELACIONES CON LOS PROVEEDORES.

Objetivo de control A.15. Protección de los Activos Accesibles a los Proveedores

Las siguientes políticas proporcionan los lineamientos para las relaciones con los proveedores asociados a los activos del módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLPRO.

7.11.1 POLPRO01. El consejo superior establecerá mecanismos de control en sus relaciones con terceras partes, que estén asociadas con los activos propios del módulo Gradebook con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

7.11.2 POLPRO02. Los empleados de la UECCI responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

7.11.3 POLPRO03. El área de informática y el área jurídica deben generar un modelo base para los acuerdos de niveles de servicio y requisitos de seguridad de la información, con los que deben cumplir terceras partes o proveedores de servicios asociados a Gradebook; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos. Así mismo deben elaborar modelos de acuerdos de confidencialidad y acuerdos de intercambio de información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

7.11.4 POLPRO04. El área de redes y datacenter de la UECCI deben establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Universidad y establecerá las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios que estén asociados al módulo Gradebook.

7.12 POLÍTICAS SOBRE LA GESTIÓN DE INCIDENTES

Objetivo de control A.16. Gestión de Incidentes y Mejoras en la Seguridad de la Información.

Las siguientes políticas proporcionan los lineamientos para la gestión de incidentes y mejoras en la seguridad de la información asociada a los activos del módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLGES.

7.12.1 POLGES01. La UECCI promoverá entre los usuarios, administradores, y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información en el módulo Gradebook y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

7.12.2 POLGES02. El consejo superior asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad en el módulo Gradebook.

7.12.3 POLGES03. El consejo Superior o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, sobre los incidentes mayúsculos que pudieran presentarse en el módulo.

7.12.4 POLGES04. El área de informática debe establecer responsables y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información asociada al módulo Gradebook. En el mismo sentido debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares

7.12.5 POLGES05. El área de informática debe crear bases de conocimiento para los incidentes de seguridad presentados en el módulo Gradebook, con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

7.12.6 POLGES06. Es responsabilidad de los empleados, docentes, estudiantes y terceros usuarios del módulo Gradebook reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos asociados al módulo con la mayor prontitud posible. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los usuarios deben notificarlo al área de informática para que se registre y se le dé el trámite necesario.

7.13 POLÍTICAS SOBRE LA CONTINUIDAD DEL NEGOCIO

Objetivo de control A.17. La Continuidad de Seguridad de la Información

Las siguientes políticas proporcionan los lineamientos para la continuidad del negocio en los activos de información del módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLCONEG.

7.13.1 POLCONEG01. El consejo superior designará y proporcionará los recursos suficientes para implementar un grupo de profesionales que conformaran el comité de continuidad del negocio para que den una respuesta efectiva a los usuarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el módulo Gradebook y que afecten la continuidad de su operación. Éste grupo responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos.

7.14 POLÍTICAS SOBRE EL CUMPLIMIENTO

Objetivo de control A.18. El Cumplimiento de Requisitos Legales y Contractuales

Las siguientes políticas proporcionan los lineamientos para el cumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad de los activos de información asociados al módulo Gradebook del sistema ARCA, los cuales se enumerarán con la sigla POLCUM.

7.14.1 POLCUM01. El departamento Jurídico debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a los activos de información del módulo Gradebook

7.14.2 POLCUM02. El área de Dirección TIC debe certificar que todo el software que se ejecuta en la UECCI esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso. Se debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en los activos de información propios de la UECCI, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

7.14.3 POLCUM03. En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la UECCI a través del departamento jurídico, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información por medio del módulo Gradebook.

Se establecerán los términos, condiciones y finalidades para las cuales la UECCI, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la Universidad, hayan suministrado datos personales.

7.14.4 POLCUM04. En caso de delegar a un tercero el tratamiento de datos personales, la UECCI exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, buscará proteger la privacidad de la información personal de sus empleados y en especial de los usuarios del módulo Gradebook, estableciendo los controles necesarios para preservar aquella información que el módulo use y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de Gradebook y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

7.14.5 POLCUM05. Los responsables de activos que procesan datos personales de administradores, estudiantes, docentes u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de Gradebook.

7.14.6 POLCUM06. Los usuarios de los portales del módulo Gradebook deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso. Los usuarios de los portales del módulo deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales del módulo.

8. CONCLUSIONES

- El módulo Gradebook toca trasversalmente a los procesos más importantes de la Universidad por lo tanto haciendo los ajustes propuestos en el plan de tratamiento de los riesgos y siguiendo las políticas propuestas se puede lograr que activos circunvecinos en la órbita de la infraestructura mejoren notablemente su estabilidad, rendimiento y seguridad.

- Se cumplió con el objetivo principal y los objetivos específicos del proyecto y en este momento las directivas de la Universidad son conscientes de todos los activos de información trasversales que toca el módulo Gradebook y gracias a MAGERIT pueden contar con herramientas base para la implementación y seguimiento al avance del mismo.

- No es posible pensar en implantar políticas de seguridad de la información sin involucrar al consejo superior, pues de hecho ellos son los principales actores en un proceso de implementación y seguimiento a las directrices allí detalladas.

- La UECCI puede, escalar los resultados a todos los activos de información teniendo en cuenta que fue necesario recorrer la totalidad de los componentes del área de informática y en caso de continuar con la metodología MAGERIT, se pueden tomar como base los hallazgos para ejecutar un plan de gestión de riesgos que abarque otros activos existentes en la organización.

- Se puede asegurar que el análisis de riesgos del módulo Gradebook permitió mostrar los altos costes que puede tener para la Universidad el no aplicar por lo menos los controles propuestos. Estos costes pueden ser incalculables como por ejemplo, la pérdida de prestigio en la comunidad educativa en caso de pérdida, o modificación de las notas de los estudiantes.

- El trabajo desarrollado basado en la optimización de los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad permitió demostrar la falta de conciencia de los elementos conformantes y que son soporte del módulo Gradebook al punto de sorprender a los mismos administradores del sistema.

- Con el análisis de riesgos desarrollado en este proyecto, la UECCI podrá emprender un plan de tratamiento de riesgos que le permitirá afrontar su defensa organizacional de manera más concienzuda y prudente, previniendo sucesos o situaciones perjudiciales y al mismo tiempo prepararse para evitar desastres en la infraestructura asociada al módulo Gradebook, así como lograr generar un plan de recuperación de desastres y de continuidad del negocio en el mediano plazo.

- Se recomienda enfáticamente a la UECCI que inicie el proceso de implementación del SGSI y se prepare para una posible certificación, pues además de las pérdidas materiales que se pueden evitar, ésta será una carta de presentación y factor diferencial en las mediciones de competitividad del ambiente educativo.

BIBLIOGRAFÍA

ABANTO, Hermes. Modelo de proyectos de tesis. 2015. Trabajo de grado. Disponible en: <http://proyectosingesistemas1.blogspot.com.co/>.

ADVISERA. S.f. ¿Qué es norma ISO 27001? [En línea]. http://advisera.com/27001academy/es/que-es-iso-27001/.

ALLEN PAULOS, John. La incertidumbre es la única certeza que hay, y saber cómo vivir con inseguridad es la única seguridad. [En línea]. <http://secureit.com.mx/gestion-de-riesgos> [citado en 15 de Noviembre de 2016].

EAR-PILAR. Entorno de análisis de riesgos: Metodología. [En linea]. http://www.ar-tools.com/es/index.html [citado en 26 de Noviembre de 2016].

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Protocolo. En: Compendio Sistema de Gestión de la Seguridad de la Información. 1 ed. Bogotá, D.C.: ICONTEC. 2006.

--------. Términos y Definiciones. En: Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2006, 3-4. p. (NTC-ISO/IEC 27001).

--------.--------. Términos y Definiciones. En: Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Bogotá D.C: ICONTEC, 2007, 3. p. (NTC-ISO/IEC 27002).

--------.--------.--------. Anexo A. En: Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2013, 13-24 p. (NTC-ISO/IEC 27001).

INTERSERVICES. S.f Cuaderno de Evaluación (Gradebook). [En línea]. <http://interservices.grupodatco.com/soluciones/campus-solutions/cuaderno-de-evaluacion/>.

ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (NORMA ISO/IEC 27000).

ISO 27002. Seguridad ligada a los recursos humanos. [En línea]. <http://www.iso27000.es/iso27002_7.html> [citado en 1 de Diciembre de 2016].

MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro I – Método. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012. 22. p.

--------. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro II – Catálogo de elementos. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012. 7. p.

--------.--------. MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En: Libro III – Guía de técnicas. Madrid: Ministerio de Hacienda y Manifestaciones Públicas, Proyectos de Análisis de Riegos, 2012.

SECUREIT–IT. Métodos de seguridad para la información digital. [En línea]. <https://www.secureit.es/metodos-de-seguridad-para-la-informacion-digital/> [citado en 2016].

UNIVERSIDAD ECCI. Artículo 35: Valoración de una asignatura o curso. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. 34. p.

--------. Artículo 45: De la seriedad de las pruebas acádemicas. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. 38. p.

--------.--------. Nuestra Misión y Visión. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. 5. p.

--------.--------.--------. S.f. Sistema Integrado de Calidad - SIC [En línea]. <http://bogota.ecci.edu.co/index.php/ecci/sistema-integrado-de-calidad>

Planteamiento de un sistema de gestión de seguridad de información en la universidad ECCI para el sistema de información académico ARCA - módulo Gradebook bajo la norma ISO 27001:2013

Cortes, Iván Darío., Torres, Osiris
dariocortes@hotmail.com; osiris.torresg@gmail.com
Universidad Piloto de Colombia

***ABSTRACT*- The present document is a synthesis of the activity developed by the authors in the ECCI University of Colombia, as a degree work to opt for the title of specialist in computer security. It proposes an information security management system under the ISO 27001: 2013 standard for the GradeBook module of its ARCA information system. In the development of the present one is made a survey of the assets associated with the GradeBook module, then runs a risk analysis and management using the MAGERIT methodology, at the end of the process, controls are proposed under ISO 27001: 2013 to mitigate the Risks encountered and as a closing point of the process, policies are generated, some of which will be included at the end of the document.**

Resumen—El presente documento es una síntesis de la actividad desarrollada por los autores en la Universidad ECCI de Colombia, como trabajo de grado para optar por el título de especialista en seguridad informática. En él se plantea un sistema de gestión de seguridad de la información bajo la norma ISO 27001:2013 para el módulo Gradebook de su sistema de información ARCA. En el desarrollo del presente se hace un levantamiento de información de los activos asociados al módulo Gradebook, luego se ejecuta un análisis y gestión de riesgos utilizando la metodología MAGERIT, al final del proceso se plantean controles bajo la norma ISO 27001:2013 para mitigar los riesgos hallados y como punto de cierre del proceso se generan políticas, de las cuales se incluirán algunas al final del documento.

Índice de Términos— Amenaza informática, SGSI Sistema de gestión de seguridad de la información, Gestión del Riesgo, Políticas de seguridad de la información

I. INTRODUCCIÓN

En el presente trabajo, se planteará un sistema de gestión de la seguridad de información para el módulo de Gradebook (libro de notas) en el sistema de información académico de la universidad ECCI (UECCI).

Este módulo (Gradebook) permite la creación de actividades que se van evaluar a los estudiantes, permitiendo el ingreso, la modificación de las notas parciales y finales por parte del docente que imparte la catedra. La importancia de este trabajo para la institución es alta debido a que dentro de la visión se evidencia lo siguiente “Seremos una universidad reconocida por su humanismo y educación tecnológica con criterios de universidad en el conocimiento, con programas pertinentes y de alta

calidad, líderes en principios y valores al servicio de la formación del capital humano" este mensaje muestra claramente como para la universidad el avance tecnológico es primordial para su constante desarrollo y crecimiento, es por ello que se busca plantear el aseguramiento de la información que se encuentra en el módulo Gradebook debido a se propone plantear controles y políticas para proteger uno de los activos más importantes de la Institución como lo son, las notas de los estudiantes y que mejor que a través de un sistema de gestión de la seguridad de la información que se encuentra relacionada directamente con las tecnologías.

II. DEFINICIÓN DEL PROBLEMA

La universidad ECCI en el año 2012 implementó un sistema académico – financiero llamado PeopleSoft - ARCA, el cual se compone de varios módulos: Comunidad del
Campus, Registro e Inscripciones, ***Gradebook***, Finanzas del Campus, Orientación Académica. Para este proyecto se va a trabajar el modulo "*Gradebook*". En este módulo el Docente registra las notas (parciales y definitivas) de las materias cursadas por los estudiantes durante un periodo académico en la Universidad.

El docente encuentra parametrizado el sistema con los tres cortes que ha estipulado la Universidad para evaluar a un estudiante, el docente solo debe realizar el cargue de notas de cada corte, las notas pueden ser cargadas dentro del rango de fechas parametrizados previamente en el sistema para la apertura y cierre de ciclo lectivo. La Pregunta es ¿Cómo mejorar la confiabilidad, integridad y disponibilidad de las notas reportadas en el sistema ARCA?

La universidad tiene estipulado los porcentajes de cada corte que se realiza en la academia para valorar los conocimientos de los estudiantes los cuales se componen de los siguientes (30% - Primer Corte, 30% - Segundo corte y 40% - tercer corte)[1], cada docente cuenta con la autonomía de asignar tantas actividades como desee para evaluar cada uno de esos cortes, pero al final de cada corte solo debe cargar una única nota. Hoy en día los docentes no entregan soporte de las notas cargadas en el sistema, aquí se ve en riesgo la integridad de la Información debido a que esta puede ser manipulada después de ser cargada y notificada en el sistema y no existe un soporte impreso o medio magnético de las notas cargas durante el periodo lectivo con el cual comparar la nota real.

III. JUSTIFICACIÓN

Actualmente la Universidad ECCI es una Institución de Educación Superior para formar profesionales íntegros, reconocidos por su lema "humanismo y educación tecnológica y con un servicio de alta calidad"[2]. Como su misión y visión lo indican uno de los temas principales es la calidad, es por eso que se debe empezar a velar por la calidad de la información que se registra, almacena y mantiene en el sistema de información Académico ARCA, para este trabajo más exactamente el registro de notas de los estudiantes que es el módulo de Gradebook.

Hoy en día UECCI, no cuenta con un sistema de gestión de seguridad de la información que garantice de forma medible la integridad y disponibilidad de la información. Teniendo en cuenta que las notas son uno de los activos de información principal de la universidad es evidente la necesidad de plantear un sistema de gestión de seguridad de información para su futura implementación en este módulo, debido a que nos permite identificar y evaluar los riesgos, las

[1] UNIVERSIDAD ECCI. Artículo 45: De la seriedad de las pruebas acádemicas. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. p. 38.

[2] UNIVERSIDAD ECCI. Nuestra Misión y Visión. En: Reglamento estudiantil. 12 ed. Bogotá D.C.: Colgraf Editores, 2015. p. 5.

amenazas y las vulnerabilidades del activo de información involucrado "las notas" de un estudiante.

El sistema de Gestión de Seguridad de la Información planteado en este proyecto se basará en la Norma ISO 27001:2013, el cual contempla entre otros los procedimientos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La UECCI actualmente se encuentra realizando gestión con la empresa Certificadora ICONTEC para realizar la capacitación al personal que pertenece al departamento de Dirección TIC en la Norma mencionada con el fin de iniciar la implementación un sistema de Gestión de Seguridad de Información en toda la Universidad, este trabajo será la base para la implementación de la Norma.

IV. MARCO TEÓRICO

Sistema de gestión de seguridad de la información (SGSI) – en ingles *Information Security Management System, ISMS).*

Se trata de una metodología enfocada hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. Nota: el sistema de gestión incluye la estructura organizacional, las políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.[3]

Antes de iniciar a explicar SGSI, se debe conocer la diferencia entre Seguridad Informática y Seguridad de Información.

- **Seguridad Informática:** Protección de las infraestructuras de las tecnologías de la información y comunicación que soportan el negocio[4].

- **Seguridad de la Información:** "Preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad"[5].

Entre los diferentes tipos de activos de información podemos encontrar los siguientes: correos electrónicos, páginas web, Bases de Datos, faxes, contratos, presentaciones, documentos entre otros. También se debe tener en cuenta el ciclo de vida de la información, lo que para la UECCI hoy es crítico, puede dejar de tener importancia con el tiempo.

La metodología permite en primer lugar realizar un inventario de activos de información relacionados con el módulo Gradebook, en segundo lugar permite realizar el análisis del riesgo y así poder identificar cual activo es más crítico (basado en las vulnerabilidades, amenazas y nivel de riesgo en el cual se encuentra), en tercer lugar se realizara un tratamiento del riesgo basados en la Norma ISO 27001:2013 trabajando los 114 controles que maneja la norma. Y por último se plantean políticas para que la universidad las pueda implementar y así pueda medir la eficacia de las medidas tomadas.

- **Gestión del riesgo:** "Son las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo"[6], este proceso permite a través del SGSI, preservar la confidencialidad, integridad y disponibilidad de la

[3] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Términos y Definiciones. En: Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2006, 3-4 p. (NTC-ISO/IEC 27001).

[4] ABANTO, Hermes. Modelo de proyectos de tesis. 2015. Trabajo de grado. Disponible en: <http://proyectosingesistemas1.blogspot.com.co/>.

[5] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Op. Cit., p. 3.

[6] Ibid.,p. 3.

misma, en el interior de la Universidad, clientes externos y diferentes entes interesados en la misma.

- **Confidencialidad: "**Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"[7].
- **Integridad: "**Propiedad de salvaguardar la exactitud y estado completo de los activos"[8].
- **Disponibilidad: "**Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada"[9].

Con el fin de proporcionar un marco de gestión de la Seguridad de la información aplicable por cualquier organización se ha creado un conjunto de estándares bajo el nombre ISO-IEC 27000, este compendio ayuda a las organizaciones a difundir, implementar las prácticas de seguridad de la información y a tomar conciencia de la importancia de proteger uno de los activos más valiosos que se tienen hoy en día, como lo es la Información[10].

Estamos en una era en que la información es el activo más preciado para nuestras empresas e incluso para nuestra vida cotidiana, se puede decir que causa más impacto en una empresa el daño de un servidor que un robo a sus instalaciones; con la inclusión de nuevas tecnologías y la masificación de la información viajando por diferentes canales, se hace evidente que el perfil de riesgos para las personas y empresas también cambia, incrementando el nivel de riesgos de la información en sus tres aspectos fundamentales: disponibilidad, integridad y confidencialidad.

Es por esto, que las empresas de ahora cuentan con áreas especializadas en la mitigación de los riesgos elaborando estrategias tales como los planes para la gestión de dichos riesgos totalmente alineados al plan estratégico del negocio.

Teniendo en cuenta este preámbulo, este proyecto se apoyó en avances de los planes de gestión de riesgos ya aplicados en algunas empresas siguiendo como directriz la norma ISO 27001:2013 la cual suministra directrices para la gestión de riesgos.

Aunque las normas ISO son el estándar internacional, no se dejaron de lado otras metodologías de análisis de riesgos, como es el caso de MAGERIT, la cual se detalla en el diseño metodológico que aplico para el desarrollo de este trabajo, esta metodología de análisis de riesgos se complementa con la norma ISO27001:2013, para la aplicación de controles relacionados en el Anexo A de la norma.

V. ESTADO ACTUAL

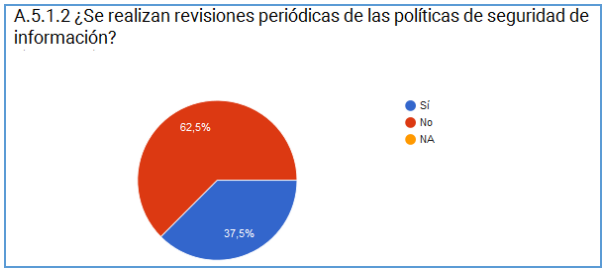
Dentro de las entrevistas realizadas a usuarios administrativos, docentes, estudiantes que tienen relación con el sistema académico y el módulo Gradebook, se evidenció que no hay lineamientos o políticas de seguridad de información para el módulo y tampoco para los activos asociados. Se cuenta con el apoyo de la alta dirección para recibir el planteamiento propuesto con fines de implementación y en general los cambios que el desarrollo del proyecto proponga. En el mismo sentido la universidad busca fortalecer los procesos que agudicen su actual certificación de calidad ISO 9001:2008 y en general las actividades que permitan fortalecer la plataforma para beneficio de los estudiantes y directivos.

A continuación, se presentan algunos resultados de las encuestas realizadas al personal que tiene relación con el módulo Gradebook en el sistema Académico, la cual se desarrolló en torno a cada uno de los controles que se encuentran en el Anexo

[7] Ibíd., p. 3.
[8] Ibíd., p. 3.
[9] Ibíd., p. 2.
[10] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Protocolo. En: Compendio Sistema de Gestión de la Seguridad de la Información. 1 ed. Bogotá, D.C.: ICONTEC. 2006.

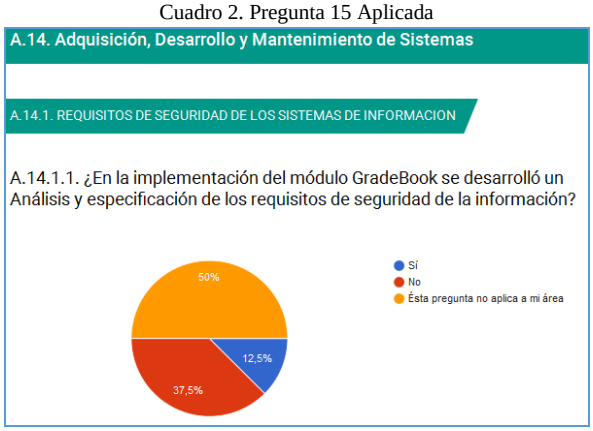
A, de la Norma ISO 27001:2013. La versión completa de estos resultados se encuentra en el trabajo de grado del cual se desprende el presente artículo[11]

Cuadro1. Pregunta 2 Aplicada



Fuente: Autores.

Cuadro 2. Pregunta 15 Aplicada



Fuente: Autores

VI. DISEÑO METODOLÓGICO

Para el desarrollo del trabajo se ha escogido la metodología de MAGERIT, debido a que cuenta con una estructura organizada para realizar el análisis y gestión de los riesgos enfocados a los sistemas de información y permite el tratamiento de control con la Norma ISO 27001:2013. Esta metodología permite hacer:

- Levantamiento de Activos
- Definición de Amenazas
- Análisis Impacto vs Probabilidad = Riesgo

VII. LEVANTAMIENTO DE ACTIVOS

Dentro del proceso de identificación fue necesario llevar a cabo las siguientes tareas que encaminaron de manera radical el proceso y ayudaron a unificar conceptos para el buen desarrollo del proyecto.
Para poder realizar la identificación de los activos se realizaron las siguientes tareas:

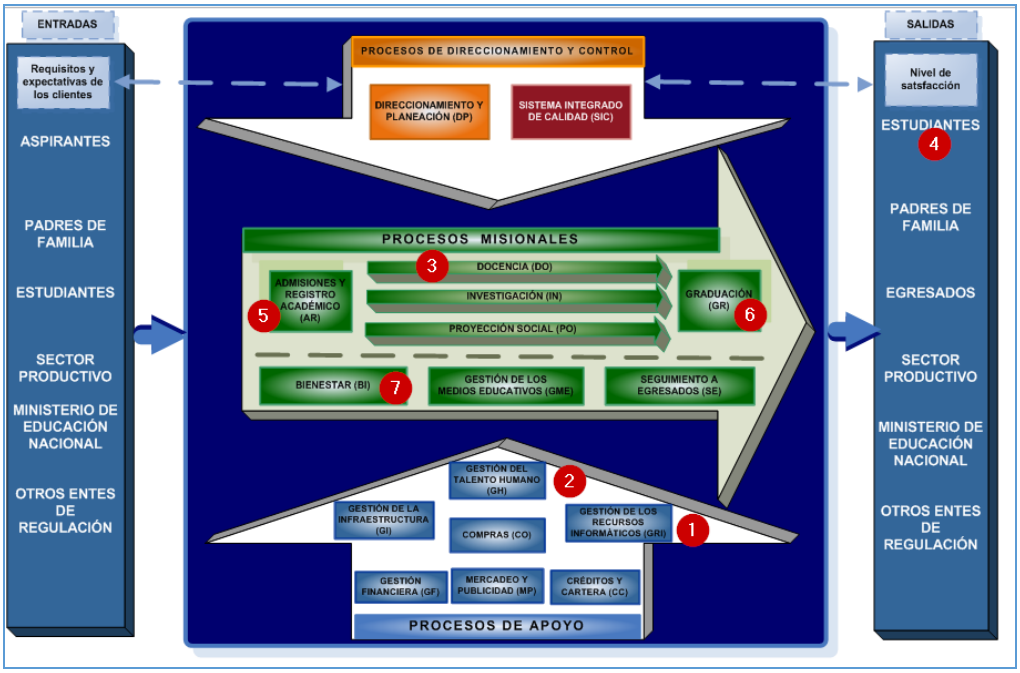
Identificar en el mapa de procesos (Ilustración 6), los procesos están relacionados con el Sistema Académico y en especial con el módulo Gradebook. Los procesos involucrados con el Modulo Gradebook del Sistema Académico son los siguientes:

- Gestión de los Recursos Informáticos - GRI
- Gestión del talento humano - GH
- Docencia - DO
- Estudiantes- ES
- Admisiones y Registro Académico - AR
- Graduación - GR
- Bienestar – BI

Dentro del proyecto se identificaron cada una de las áreas que son propietarias y custodias de los activos de Información hallados en cada uno de los procesos anteriormente mencionados que se encuentran relacionados con el Módulo Gradebook. Generando unas tablas como las siguientes:

[11] CORTES, TORRES (2.016) Universidad Piloto de Colombia Planteamiento de un sistema de gestión de seguridad de información en la universidad ECCI para el sistema de información académico arca - módulo Gradebook bajo la norma ISO 27001:2013

Ilustración 1. Mapa de Procesos UECCI[12]



Fuente: Autores.

Tabla 1 . Descripción de Custodio – GH

Tipo de Proceso	Propietario de la Información	Custodio de la Información
Apoyo	**Gestión del Talento Humano**	Jefe de Gestión Humana. Auxiliar de selección. Personal.

Fuente: Autores.

Tabla 2. Descripción de Propietario – DO

Tipo de Proceso	Procesos	Propietario
Misional	**Docencia**	**Docente:** Verificar, Mantener la Integridad, confidencialidad y disponibilidad de las notas. **Coordinador:** Verificar, mantener la Integridad, Confidencialidad y Disponibilidad de las notas.

Fuente: Autores.

[12] UNIVERSIDAD ECCI. Sistema integrado de calidad – SIC, Op. cit. p. 1.

Asignación de Propietarios y Custodios al inventario de Activos. Luego de haber identificado los propietarios de cada proceso procedemos a asignar propietarios y custodios a cada uno de los activos.

El listado completo de las tablas (5 en total) se encuentran detalladas en el proyecto, CORTES, TORRES (2.016) Universidad Piloto de Colombia Planteamiento de un sistema de gestión de seguridad de información en la universidad ECCI para el sistema de información académico arca - módulo Gradebook bajo la norma ISO 27001:2013

Tabla 3. Activos de GRI (1)

Información Basica del Activo						Propiedad del Activo	
ID	Proceso	Nombre del activo	Descripción / Observaciones	Magerit V3 Tipo_Activo	Ubicación	Propietario	Custodio
A1	Gestión de los Recursos Informáticos	Equipos de Computo Docentes, Administrativos y estudiantes	Distribuidos en áreas administrativas, salas de docentes y salas de sistemas de estudiantes	AHW	En toda la Organización	Soporte Informático	Auxiliar o Técnico de Soporte
A2		Licencias de Sistemas Operativos Windows	Distribuidos en áreas administrativas, salas de docentes y salas de sistemas de estudiantes	ASW	Sede C, Primer Piso - área de Soporte Informático	Soporte Informático	Auxiliar o Técnico de Soporte
A3		Licencias para Servidores Oracle	Distribuido en el servidor donde se encuentra la base de datos, la aplicación y el los equipos de computo asignados a los adminsitradores de la aplicación web y el DBA	ASW	Sede C, Primer Piso - área de Soporte Informático	Soporte Informático	Auxiliar o Técnico de Soporte
A4		Sistema de Información PeopleSoft - ARCA	Distribuida en areas administrativas y salas de Docentes y via web	ASW	Sede D, 4to piso en Datacenter	Datacenter	Ing. Electronico/Ing. Sistemas
A5		Manuales de Usuario	Manual que describe toda la navegación que puede realizar un usuario según su rol asigando en Gestión Humana	AS	Sede C, 1er. Piso - área de Informática y vía web	Informática	Auxiliar de Informática
A6		Manual de Perfiles en ARCA	Manual que desarrollo el área de Informática para asignar perfiles en el sistema ARCA según las reponsabilidades dentro de la organziación	AS	Sede C, 1er. Piso - área de Informática	Inofrmática	Auxiliar de Informática
A7		Routers y Switch	Estan asignados en varias sedes de la Organización	ACOM	En toda la Organización	Redes	Técnico de Redes
A8		Modem	Estan asignados en varias sedes de la Organización	ACOM	En toda la Organización	Redes	Técnico de Redes

Fuente: Autores.

VIII. ANÁLISIS Y GESTIÓN DEL RIESGO BAJO METODOLOGÍA MAGERIT V 3.0

Después de la clara identificación de cada uno de los activos del módulo GradeBook, se procede a realizar el análisis y gestión del riesgo bajo la Metodología MAGERIT.

Amenazas vs Activos. Para analizar los activos versus las amenazas se debe tener en cuenta el listado de categorías de amenazas identificado en el marco teórico en capítulo 4.1.1 de este trabajo. A continuación, se presentan las amenazas vs cada uno de los activos del inventario.

Tabla 4. Cruce Amenazas vs Activos

	ACTIVOS VS AMENAZAS																				
AMENAZA/ACTIVO	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22
AM1 - Desastres Naturales - Fuego	X									X	X	X		X	X							
AM2 - Desastres Naturales - Daños por agua	X									X	X	X		X	X							
AM3 - Desastres Naturales - Desastres naturales	X									X	X	X		X	X							
AM4 - De Origen Industrial -	X									X	X	X		X	X							
AM5 - De Origen Industrial - Daños por agua	X									X	X	X		X	X							
AM6 - De Origen Industrial - Desastres industriales	X									X	X	X		X	X							
AM7 - De Origen Industrial - Contaminación mecánica	X									X	X	X		X	X							
AM8 - De Origen Industrial - Contaminación																						
AM9 - De Origen Industrial - Avería de origen físico o lógico	X	X	X	X	X	X				X	X	X	X	X	X							
AM10 - De Origen Industrial - Corte del suministro eléctrico	X									X	X	X		X	X							

Fuente: Autores.

Estimación del riesgo. La gestión del riesgo que se plantea para el módulo de Gradebook (Libro de Notas) en el sistema de Información Académico, es un procedimiento que se usa para valorar cada uno de los activos de información que se relacionan con el módulo a través de la aplicación de la metodología MAGERIT, esta metodología permite identificar los activos, las amenazas que le afecta a cada uno de ellos y cuenta con una escala cualitativa de estimación del riesgo según el impacto y la probabilidad que le aplique a cada activo vs amenaza, en este trabajo se identificaran riesgos ***críticos, importantes, apreciables, bajos y despreciable***[13],

Tabla 5 Cruce Amenazas vs activos

Estimación Riesgo	
	Crítico
	Importante
	Apreciable
	Bajo
	Despreciable

Fuente: Autores.

en la tabla 5 se presenta la escala cualitativa de estimación del riesgo y los riesgos que se encontraron son los siguientes:

Se evaluaron los activos versus las amenazas y se obtuvieron los siguientes resultados:

Se evaluaron 56 amenazas (Cap. 4.1.1) por 22 activos que se lograron levantar en el inventario de Activos (Cap. 5.2.3), el cruce de esta información se realizó con ayuda del departamento de calidad, administrativos, docentes y estudiantes, los resultados arrojados han permitido evidenciar que la universidad no cuenta con un sistema de gestión de seguridad de información para ninguno de los activos encontrados y tampoco se presenta evidencia de políticas de seguridad para el sistema de Información Académico.

A continuación, se presenta un resumen general de cuantos riesgos se encontraron.

[13] MINISTERIO DE HACIENDA Y MANIFESTACIONES PÚBLICAS, PROYECTOS DE ANÁLISIS DE RIEGOS. MAGERIT – Versión 3.0: Metodología de análisis y gestión de Riesgos de los sistemas de información. En: Libro II – Catalogo de elementos, Op. cit. p. 7.

Tabla 6. Estimación del Riesgo (todos los Activos ECCI vs Amenazas MAGERIT)

Estimación del Riesgo					
Impacto/probabilidad	**MB**	**B**	**M**	**A**	**MA**
MA	6	24	53	22	1
A	10	30	59	18	2
M	10	27	20	12	2
B	16	1	1	4	1
MB	2	0	0	0	0
Total de Riesgos	**321**				

Fuente: Autores.

Se puede evidenciar que se logró encontrar un total de 321 riesgos que se presentan para el módulo Gradebook, afectando no solo el sistema de información (ASW), el servidor de Base de Datos (AHW), los servicios ofrecidos (AS) y no dejando atrás el personal (Docente, Administrativo, Estudiante), como se puede ver el sistema está compuesto por un todo que tiene varias partes, las cuales sino se protegen el daño de cualquiera de ellas puede afectar el buen funcionamiento del módulo), por ello es importante empezar a plantear políticas de seguridad que permitan mitigar cada uno de estos riesgos en especial los críticos e importantes, pero para el proyecto se trabajarán solo los Críticos (se encontraron 120) y la Universidad asume el trabajo de los importantes (109), apreciables (62), bajo (12) y despreciables (18).

Ahora se presentan los riesgos por Activo vs Criticidad, para verificar cual es el activo que más se está afectando en este momento y que es importante plantear políticas para su óptimo funcionamiento y cuidado.

Tabla 7. Criticidad Riesgo vs Tipo_ Activo

Riesgo / Tipo_ Activo	ASW	AS	AP	AHW	ACOM
Crítico	49	----	21	34	16
Importante	18	----	12	58	21
Apreciable	17	10	1	27	7
Bajo	----	2	2	7	1
Despreciable	----	16	----	2	----

Fuente: Autores.

De la tabla 7 lo que se puede concluir es que los activos más afectados en primer lugar son el Software, El hardware y el personal, todos estos activos son muy importantes para el correcto funcionamiento no solo del módulo Gradebook sino del sistema de información académico, se plantearan políticas y controles para que al momento de implementarlos se pueda mitigar el riesgo y se mejore la seguridad del sistema de información académico, y brindar así Confidencialidad, Disponibilidad e Integridad. En el análisis del riesgo se encontraron 120 riesgos críticos que son afectados por las diferentes amenazas categorizadas según MAGERIT Cap. (4.1.1).

El impacto de estos riesgos críticos puede causar:

- Interrupción de actividades

- Sanciones por no cumplir con la norma.
- Desventaja Competitiva.
- Pérdida de Imagen.
- Destrucción y perdida de activos relacionados con el módulo Gradebook.

A continuación, se especifican los riesgos que se van a tomar para trabajar en esta fase del proyecto.

- No se cuenta con una base de conocimiento de los casos que se pueden presentar para incidencia en los equipos de cómputo, por lo tanto, cada técnico de soporte resuelve el servicio de forma distinta según su experiencia y conocimiento, en ocasiones la solución puede ser exitosa pero no la más eficiente y la más eficaz, por lo tanto, se debe crear una base de conocimiento donde se documenten las incidencias para poder normalizar todos los procesos técnicos.
- No se cuenta con restricciones para dispositivos de almacenamiento USB, aunque se cuenta con un sistema de protección contra virus para mitigar los riesgos de contagio de virus, las unidades de almacenamiento de USB pueden fácilmente afectar a un Sistema de Información.
- La UECCI cuenta con licencias legales gracias a la compra de licencias perpetuas o renovaciones anuales para sus equipos de cómputo, los desarrollos que se realicen dentro de la institución están licenciados sin embargo se evidencia un gran problema y es que no se cuenta con un control.para la instalación de software Ilegal, o la debida autorización del personal de Soporte Informático.

Tabla de Riesgos Críticos. El resto de tablas generadas y explicación completa se puede consultar en [1] Algunos de los puntos encontrados son:

- Aunque se cuenta con personal para realizar el mantenimiento del hardware de tipo preventivo, correctivo y predictivo en los diferentes equipos de cómputo no se cumple con el cronograma de mantenimiento propuesto a inicio del año lectivo debido a las fechas de terminación del contrato.
- No se cuenta con un plan de tratamiento para la baja de equipos, cuando se actualizan o se cambian, solo se realiza formateo para entregar al siguiente usuario si el equipo sigue en uso, se saca un backup de la información privada de las máquinas y se sube a la nube, pero no se cuenta con una política de seguridad de la información que reposa en la nube.
- No se cuenta con un procedimiento para la actualización de parches de seguridad o software en los sistemas críticos de la Universidad.
- En el Firewall se presentan cuellos de botella debido a que hoy en día se está manejando la virtualización de computadores, para mitigar este riesgo se recomienda mejorar equipos de comunicación.
- Existen reglas de protección de acceso a los firewalls desde la red externa a servicios y servidores específicos en la red de servidores DMZ (Desmilitarizada), sin embargo, se evidencia que en la red inalámbrica se puede tener acceso a través de los puertos abiertos a servicios restringidos

Tabla 8. Riesgos Críticos a Trabajar (1)

Nº Riesgo	Activo	Amenaza	I	P	Riesgo	Tipo_Activo
9	Equipos de Computo Docentes, Administrativos y estudiantes	AM10 - De Origen Industrial - Corte del suministro eléctrico	MA	M	Crítico	AHW
12	Equipos de Computo Docentes, Administrativos y estudiantes	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	A	Crítico	AHW
15	Equipos de Computo Docentes, Administrativos y estudiantes	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	M	Crítico	AHW
16	Equipos de Computo Docentes, Administrativos y estudiantes	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	Crítico	AHW
17	Equipos de Computo Docentes, Administrativos y estudiantes	AM38 - Ataques Intencionados - Uso no previsto	MA	M	Crítico	AHW
21	Equipos de Computo Docentes, Administrativos y estudiantes	AM51 - Ataques Intencionados - Robo	MA	M	Crítico	AHW
26	Operativos Windows	Difusión de software dañino	MA	M	Crítico	ASW
30	Operativos Windows	Fugas de información	MA	M	Crítico	ASW
36	Operativos Windows	software dañino	MA	M	Crítico	ASW
37	Operativos Windows	secuencia	MA	M	Crítico	ASW
38	Operativos Windows	autorizado	MA	M	Crítico	ASW
39	Operativos Windows	deliberada de la información	A	A	Crítico	ASW
40	Operativos Windows	de información	MA	A	Crítico	ASW
41	Operativos Windows	de información	MA	A	Crítico	ASW
42	Operativos Windows	Manipulación de programas	MA	M	Crítico	ASW
46	Oracle	Difusión de software dañino	MA	M	Crítico	ASW
50	Oracle	Fugas de información	MA	M	Crítico	ASW
56	Oracle	software dañino	MA	M	Crítico	ASW
57	Oracle	secuencia	MA	B	Crítico	ASW

Fuente: Autores.

Tabla 9. Amenazas que Afectan el Hardware de los Riesgos Críticos Parte (1)

Nº Riesgo	Activo	Amenaza	I	P	Riesgo	Tipo_Activo
9	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM10 - De Origen Industrial - Corte del suministro eléctrico	MA	M	Crítico	AHW
12	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM20 - Errores y fallos no intencionados - Deficiencias en la organización	MA	A	Crítico	AHW
15	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM32 - Errores y fallos no intencionados - Pérdida de equipos	MA	M	Crítico	AHW
16	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM37 - Ataques Intencionados - Abuso de privilegios de acceso	MA	M	Crítico	AHW
17	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM38 - Ataques Intencionados - Uso no previsto	MA	M	Crítico	AHW
21	Equipos de Cómputo Docentes, Administrativos y estudiantes	AM51 - Ataques Intencionados - Robo	MA	M	Crítico	AHW

Fuente: Autores.

Tabla 10. Activo amenazas vs controles ISO 27001:2013

A3 - Licencias para Servidores Oracle	
Amenazas	**Descripción del Control aplicado de la Norma ISO 27001:2013**
AM21	**A.12.5.1 Instalación de software en sistemas operativos**
AM27	**A.12.4.2 Protección de la información del registro**
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación
AM39	**A.12.2.1 Controles contra códigos maliciosos**
AM41	**A.12.1.1 Procedimientos de operación documentados**
	A.12.1.2 Gestión de cambios
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM42	**A.16.1.2 Reporte de eventos de seguridad de la información**
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM45	**A.13.1.2 Seguridad de los servicios de red**
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM46	**A.12.2.1 Controles contra códigos maliciosos**
	A.12.3.1 Respaldo de la información
AM47	**A.12.3.1 Respaldo de la información**
AM48	**A.12.5.1 Instalación de software en sistemas operativos**
	A.12.6.2 Restricciones sobre la instalación de software

Fuente: Autores

IX. PLANTEAMIENTO DE LOS CONTROLES QUE SE DEBEN APLICAR BAJO LA NORMA ISO 27001:2013 A LOS RIESGOS ENCONTRADOS EN EL ANÁLISIS

En el siguiente aparte se encuentra relacionado cada uno de los controles que se plantean aplicar en cada uno de los riesgos críticos trabajados en el proyecto. Se encuentra cada Activo con su amenaza y el control que puede aplicar bajo la norma ISO 27001:2013.

Tabla 10. Activo amenazas vs controles ISO 27001:2013

A3 - Licencias para Servidores Oracle	
Amenazas	**Descripción del Control aplicado de la Norma ISO 27001:2013**
AM21	**A.12.5.1 Instalación de software en sistemas operativos**
AM27	**A.12.4.2 Protección de la información del registro**
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación
AM39	**A.12.2.1 Controles contra códigos maliciosos**
AM41	**A.12.1.1 Procedimientos de operación documentados**
	A.12.1.2 Gestión de cambios
	A.12.3.1 Respaldo de la información
	A.12.4.1 Registro de eventos
	A.12.4.2 Protección de la información del registro
	A.12.4.4 Sincronización de relojes
AM42	**A.16.1.2 Reporte de eventos de seguridad de la información**
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM45	**A.13.1.2 Seguridad de los servicios de red**
	A.16.1.2 Reporte de eventos de seguridad de la información
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
	A.16.1.5 Respuesta a incidentes de seguridad de la información
	A.16.1.7 Recolección de evidencia
AM46	**A.12.2.1 Controles contra códigos maliciosos**
	A.12.3.1 Respaldo de la información
AM47	**A.12.3.1 Respaldo de la información**
AM48	**A.12.5.1 Instalación de software en sistemas operativos**
	A.12.6.2 Restricciones sobre la instalación de software

Fuente: Autores.

Tabla 11. Control explicado para el activo 1

A1 - Equipos de Computo Docentes, Administrativos y estudiantes		
Nº Control	**ISO 27001:2013**	**Descripción del control a aplicar**
C1	A.8.1.1	Se deben identificar los activos de la universidad relacionados con el modulo Gradebook que estan asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos.
C2	A.8.1.2	Todos los Activos mantenidos en el inventario deben tener un propietario.
C3	A.8.3.2	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
C4	A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el tranporte.
C5	A.9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (especial en gradebook).
C6	A.9.1.2	Solo se debe permitir acceso a la red y a los servicios a las los cuales hansido autorizados. (Basados en el rol para el cual fue contratada a persona).
C7	A.9.2.1	Se debe implmentar un proceso formal de Registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
C8	A.9.2.3	Se debe restringir y controlar la asignacion y uso de derechos de acceso privilegiado (ej: Coordinador, Secretaria Gral, Decanos).
C9	A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo o se deben ajustar cuando se realicen cambios.
C10	A.11.2.2	Los equipos se deben proteger contra fallas de energía y otras interrupciones casusadas por fallas en los servicios de suministros), ej: Pararayos.
C11	A.11.2.8	Los usuarios deben asegurarse de que a los equipos desatendidos se les de protección apropiada.
C12	A.12.1.1	Los procesos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
C13	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio ej: (cambio de % en notas parciales), en las instalaciones (datacenter) y en los sistemas de procesmiento de información (ARCA) que afectan la seguridad de la información.

Fuente: Autores.

X. POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LOS ACTIVOS MÁS SIGNIFICATIVOS DEL MÓDULO GRADEBOOK EN EL SISTEMA ACADÉMICO

Las políticas de Seguridad de la Información, serán las directrices que deben cumplir los usuarios, administradores y terceros que hacen uso del módulo Gradebook del sistema Arca UECCI, y demás custodios de los activos asociados, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad de la información generada.

Están orientadas a proteger los activos de información en todos los ambientes, internos y externos, en los cuales se almacenan, procesan, transmiten, operan o usan y procuran mantener los Por lo anterior, se proponen las siguientes Políticas Generales en Seguridad de la Información, basados en la norma ISO 27001:2013, las cuales ayudarán a ofrecer la información del sistema de notas de manera segura y confiable.

Estas políticas deben ser informadas, socializadas y promovidas como de estricto cumplimiento para los actores asociados a los activos definidos en la fase inicial de éste proyecto.

A continuación, algunos ejemplos de políticas planteadas

7.1 POLÍTICAS GENERALES

Objetivo de control A.5. Políticas de seguridad de la Información.

7.1.1 POLGRAL001. Los directivos del departamento TIC evaluarán las situaciones que hayan dado lugar a un incumplimiento a las Políticas de Seguridad de la Información, recomendará las acciones a seguir, para mantener el Modelo de Seguridad de la Información propuesto para el módulo Gradebook. En el mismo sentido será el encargado de aprobar modificaciones o nuevas políticas de seguridad de la información.

ASIGNACIÓN DE RESPONSABILIDADES

Objetivo de control A.6. Organización de la seguridad de la información

Las siguientes políticas describen los roles y responsabilidades de los usuarios del módulo Gradebook los cuales se enumerarán con la sigla POLRES:

7.2.1 POLRES01. Consejo superior Es el responsable que los usuarios a su cargo, conozcan y apliquen las políticas de seguridad de la información. En ese sentido deben exigir que todo administrador, usuario o terceras partes que tengan acceso a los activos de información del módulo Gradebook, cumplan las políticas y los procedimientos de seguridad de la información establecidos por el módulo Gradebook del sistema Arca UECCI.

CONCLUSIONES

- El módulo Gradebook toca trasversalmente a los procesos más importantes de la institución educativa por lo tanto haciendo los ajustes propuestos en el plan de tratamiento de los riesgos y siguiendo las políticas propuestas se puede lograr que activos circunvecinos en la órbita de la infraestructura mejoren notablemente su estabilidad, rendimiento y seguridad.

- Se puede asegurar que el análisis de riesgos del módulo Gradebook permitió mostrar los altos costes que puede tener para la Universidad, el no aplicar por lo menos los controles propuestos. Estos costes pueden ser incalculables como por ejemplo la pérdida de prestigio en la comunidad educativa en caso de pérdida, o modificación de las notas de los estudiantes.
- Se recomienda enfáticamente a la UECCI que inicie el proceso de implementación del SGSI y se prepare para una posible certificación, pues además de las pérdidas materiales que se pueden evitar, ésta será una carta de presentación y factor diferencial en las mediciones de competitividad del ambiente educativo.

REFERENCIAS

[1]ABANTO, Hermes. Modelo de proyectos de tesis. 2015. Trabajo de grado. Disponible en: <http://proyectosingesistemas1.blogspot.com.co/>.

[2]ADVISERA. S.f. ¿Qué es norma ISO 27001? [En línea]. Http://advisera.com/27001academy/es/que-es-iso-27001/.

[3]ALLEN PAULOS, John. La incertidumbre es la única certeza que hay, y saber cómo vivir con inseguridad es la única seguridad. [En línea]. <http://secureit.com.mx/gestion-de-riesgos> [citado en 15 de noviembre de 2016].

[4]EAR-PILAR. Entorno de análisis de riesgos: Metodología. [En línea]. Http://www.ar-tools.com/es/index.html [citado en 26 de noviembre de 2016].

AUTORES

Ing. Osiris Torres Gutierrez
osiris.torresg@gmail.com

Nacida el 16 de Agosto de 1982, Estudios realizados Profesionales Universidad Distrital Francisco Jose de Caldas, Ingeniera de Sistemas, 2013 - Cursos realizados Linux, 2008, SENA - Tutor en Ambientes Virtuales de aprendizaje Moodle, 2008, SENA - Sistemas de Información en las Organizaciones, 2008, SENA - Documentación de un Sistema de Gestión de Calidad ISO 9000:2008,2008, SENA - Fundamentos del Sistema de Gestión de Calidad ISO 900:2008,2008, SENA - Formación de Auditores de Sistemas de Gestión de la Calidad, Técnicas de Auditoria, 2008, ICONTEC - Auditoria Informática: Conceptualización, 2009, SENA - Indicadores de Gestión, 2010, ICONTEC - Diseño y Creación de Páginas Web (Básico), 2010, Universidad ECCI - Creación de empresas y Plan de Negocios, 2010, Universidad ECCI - Control Interno en los Sistemas de Informáticos, 2011, SENA - Formación de Auditores en Sistemas de

Gestión de la Calidad de la Investigación, Desarrollo e Innovación I+D+i, 2014, ICONTEC - Ingles A2, 2015, Universidad ECCI - Gestión de la Seguridad Informática, 2015, SENA - Controles y Seguridad Informática, 2015, SENA.

Ella ha laborado desde el 2008 hasta la actualidad en la Universidad ECCI desempeñando las siguientes funciones: Administrar base de datos (Oracle, MySQL, Postgresql), administración de Pagina Web, administración de correo, auditoria interna (ISO 2008-9001 e I+D+i). Implementación de Sistema de Información Académico y financiero (PeopleSoft), en los módulos PeopleSoft Financials, PeopleSoft Campus Solutions. Capacitación de los Usuarios (Peoplesoft), Administración de Sistema Contable y Administrativo - SIIGO. Administración de Sistemas de Información "Sistema Nacional de Información de la Educación Superior (SNIES) y Sistema para la Prevención de la Deserción en las Instituciones de Educación Superior (SPADIES) dentro de la Universidad ECCI. Desarrollo de Manuales técnicos y funcionales (PeopleSoft). Documentación de los procesos realizados en el área TIC. Actualmente (2.016) está culminando la especialización en seguridad informática en la Universidad Piloto de Colombia

Ing. Iván Darío Cortes MCP
dariocortes@hotmail.com

Terminó sus estudios de Ingeniería de sistemas en la universidad Nacional de Colombia en el 2.005 en donde además de culminar con éxito las labores académicas desarrollo actividades de investigación en el grupo Unidades de Desarrollo. Su tesis de pregrado estuvo basada en PLT específicamente en la trasmisión de datos enfocados a la trasmisión de televisión por medio de líneas Eléctricas. Desarrolló múltiples certificaciones de la casa Microsoft específicamente en el área de usuario final, servidores de control de domino e ISA server. Actualmente trabaja en el sector privado y su empresa presta servicios de consultoría en el área de IT a empresas del sector de distribución de combustibles, licitaciones con el estado y consultorías contables. Actualmente (2.017) está culminando la especialización en seguridad informática en la Universidad Piloto de Colombia